Solving Crime Without Breaking Encryption

A Three-page Summary

June 2026

Introduction: The False Choice

Policymakers are often presented with a dangerous dilemma: either we break encryption to catch criminals, or we let the Internet "go dark." This is a false choice.

Law enforcement agencies do not need to break the digital safety of billions of users to investigate crimes effectively. We are living in the golden age of digital evidence; agencies have access to more data today—location history, metadata, and transaction logs—than ever before.

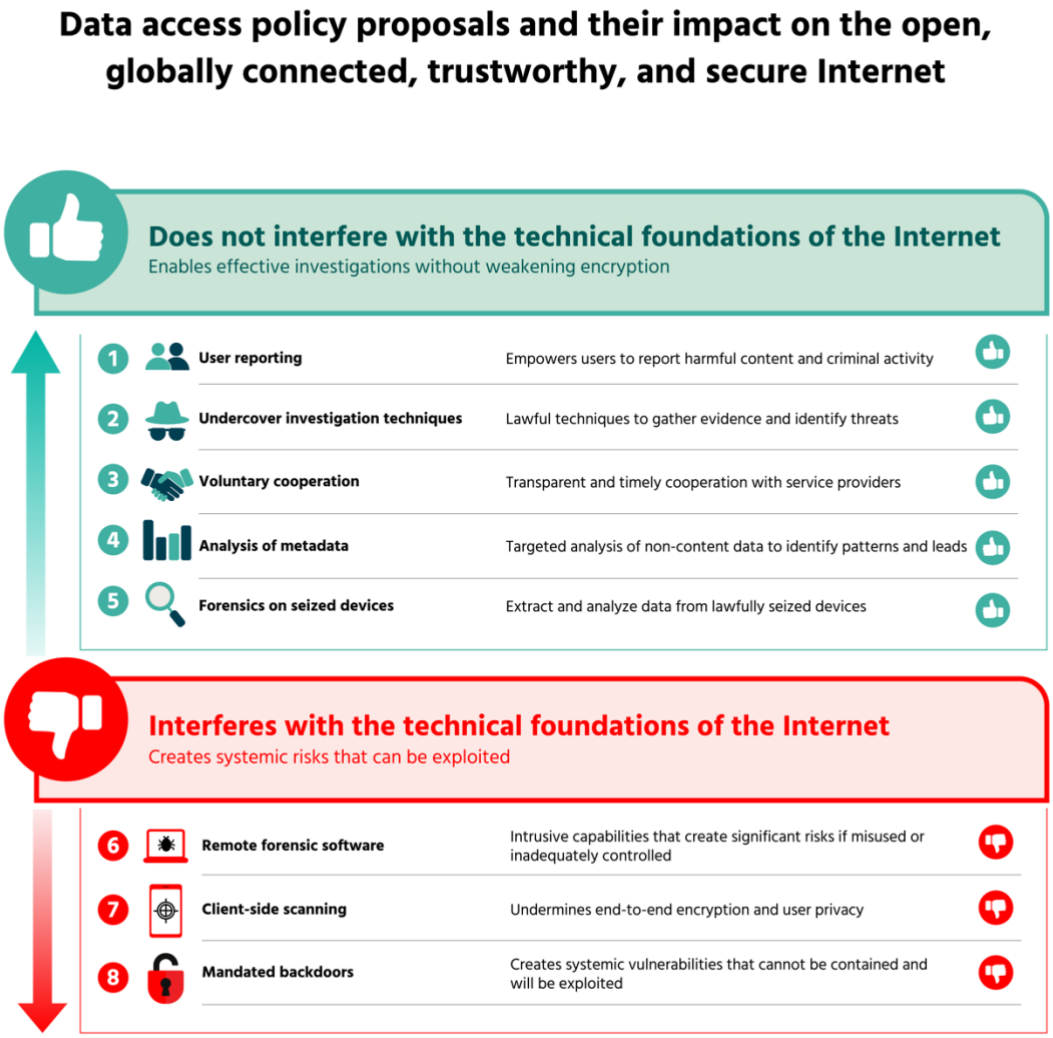
Breaking encryption—through backdoors, client-side scanning, or mandated access—fails the legal tests of necessity and proportionality. It introduces systemic vulnerabilities that criminals and hostile states will exploit, making everyone less safe.

The Solution: Effective Tools (Support These)

Instead of demanding "magic keys," governments should resource and legalize these effective investigative methods:

- **User reporting**: Important evidence can often be obtained directly from witnesses, victims, or cooperating individuals involved in criminal activity. Provide easy-to-use mechanisms for user-reported crime and for recovering digital evidence from devices.
- **Undercover operations for covert and serious crimes such as CSAM**: Traditional policing adapted for the digital age—such as infiltrating groups and using decoy accounts—remains the gold standard for catching predators.
- **Voluntary cooperation**: Fast, reliable channels for platforms to share non-content data (login history, account activity) solve more crimes than mandated technical weaknesses.
- **Metadata analysis**: Encryption protects content, not behavior. Investigators can build timelines, map criminal networks, and identify suspects using non-content data (who, when, where) without decrypting messages. This measure does not imply a call for blanket collection and retention of any such information about every user.

- Digital forensics on seized devices: Accessing data physically stored on a suspect's seized device is a targeted alternative to mass surveillance. It accesses evidence at the endpoint, leaving the secure "pipe" intact for the rest of the world.



The Red Zone: Dangerous Proposals (Reject These)

- Mandated Backdoors: Intentionally inserting weaknesses into software.
- Client-Side Scanning: Turning user devices into surveillance tools.
- "Lawful Access by Design": A marketing term for systemic vulnerabilities.

The Bottom Line: Protecting strong encryption is not an obstacle to public safety—it is a prerequisite for it. Policymakers must stop looking for a technical backdoor and start investing in the human and forensic capabilities that solve crime.

Recommendations

Policy responses to serious crime in the digital environment should be grounded in the following principles:

- **Preserve strong encryption**: Encryption is essential to maintaining the confidentiality, integrity, and authenticity of data and communications. It underpins a secure and trustworthy Internet and protects individuals, businesses, governments, and critical infrastructure. Policies should strengthen, not weaken, encryption.
- **Ensure necessity and proportionality**: Investigative measures must be targeted, lawful, and limited to what is strictly necessary and proportionate to the seriousness of the crime. Measures that undermine the security of all users in order to investigate a limited number of cases fail this test and should not be pursued.
- **Support a secure and trustworthy Internet**: Policy and operational approaches must align with the goal of a resilient Internet that protects data confidentiality, integrity, and availability. Maintaining strong cybersecurity across the digital ecosystem is essential for public safety, economic stability, and trust in digital services.