Intermediaries and Encryption

Pressuring Intermediaries to Weaken Security is Not the Answer to Preventing Harmful Content Online

August 2022

The Internet is a powerful tool that connects people around the world, informs them, and helps them do business. It offers virtually unlimited potential for people to innovate, improve their quality of life, celebrate, learn from diversity, and tackle the world's most complex challenges. Unfortunately, it is also sometimes used to enable or commit crimes and to spread dangerous misinformation and hate speech online. In extreme cases, it has been used to broadcast or incite actions that have led to physical harm.

Some governments have suggested that such bad behavior can be prevented by making Internet intermediaries liable for what their users publish or share online.1 Certain governments have already indicated that intermediaries, such as social media platforms and end-to-end encrypted messaging services, could be held liable2 if they are not able to "trace" (i.e. identify the originator of) content shared via their platforms. Such proposals are unlikely to achieve their stated goals and will weaken the security tools we rely on daily to protect people, businesses, economies, and nations from harm.

Practical Risks and Challenges

Breaking encryption breaks trust and security: As noted above, some governments want "traceability", even for end-to-end encrypted messages between parties who wish to communicate confidentially. Governments want to be able to determine whether a specific message is offensive or illegal and whether it originated from a specific user. To do this, intermediaries would need access to one or more of the following:

- The unencrypted message is on the sender's device.
- The decrypted message is on the recipient's device.
- The encrypted message, and the means to decrypt it.

---

1 Examples include the Amendments to India's Information Technology (Intermediaries Guidelines) Rules under the Information Technology Act.

2 The legal basis for liability (or exemption from it) may vary by jurisdiction. For instance, in India, it is covered by Section 79 of the IT Act of 2000: https://cis-india.org/internet-governance/resources/section-79-information-technology-act while for intermediaries in the United States it comes under Section 230 of the Communications Decency Act 1996: https://en.wikipedia.org/wiki/Section_230_of_the_Communications_Decency_Act

This would mean they are either bypassing or overriding the encryption of the message, and therefore its confidentiality.

> **Impact:** Traceability breaks the principle of confidential communication and undermines user trust in platforms and service providers that use these methods to access the content. Ultimately, if encryption is flawed by design (including intentional "back doors", "silent listeners", or mandated government keys), users can no longer trust the confidentiality or integrity of their online communications. This breaks fundamental functions we rely on daily to secure devices, data, and transactions, and thus to keep people, economies, infrastructure, and workplaces safe.

It is not helpful to legislate for the impossible: Some governments are trying to make dangerous proposals appear uncontroversial by stating only the desired *outcome*, rather than the measures that would be needed to make that outcome happen. For instance, requiring intermediaries to guarantee the safety of children online, but not stating how they expect this to be achieved.

However, by framing the issue as one of information being "inaccessible to law enforcement", they are implying that the problem is encryption, and the solution is to bypass or override it. At least one current proposal claims that such a solution can be deployed without undermining the security or trust of legitimate services and users. The Internet Society continues to believe this is simply not the case, and in May 2019, it was one of almost 50 signatories to an open letter setting out the risks and shortcomings of such an approach.3

> **Impact:** However well-intentioned it is, any law that results in weakened security mechanisms increases the opportunity for malicious activity and puts legitimate users and services at risk. This includes law enforcement and other government agencies.

Regardless of how the goal is framed and phrased in the law, the response of the technical community has been clear and consistent: you cannot design an encryption bypass or override that "only the good guys can use".4 This is not dogmatic thinking on the part of the technical experts: it is based on the fundamental, mathematical reasons that make good encryption systems good. You cannot have a reliable encryption system that is simultaneously strong against some attackers but weak against others. You cannot have a robust encryption system that is robust except when you want it to be weak.

Mandating user authentication adds cost and complexity: To help identify the originators of illegal content, some countries are tempted to insist that users must authenticate to access any online

3 https://regmedia.co.uk/2019/05/30/letter_to_gchq_ghost_user_cryptobusting_plan.pdf

4 https://mitpress.mit.edu/blog/keys-under-doormats-security-report

service.5 This may sound simple, but reliable authentication is hard to achieve even when it is in the user's interest (for instance, for ATM cash withdrawals). When the user has an incentive to avoid identification, it is even harder. Approaches that rely on users authenticating with official identity documents (driver's license, passport, government electronic ID) are complex and costly and depend for their reliability on a host of technical and non-technical factors including reliable processes for issuing and revocation, tamper resistance, identity, and access management, and so on. In most cases, adding biometrics worsens this complexity.

What's more, other 'exceptional access' proposals are based on undermining the very authentication protocols on which reliable encryption depends6. If you cannot be sure that only the intended recipient can access the keys to decrypt your message, you cannot be sure of its confidentiality.

> **Impact:** Proposals based on compulsory authentication increase cost and inconvenience without necessarily achieving the stated goal. Policy proposals in this area appear to have conflicting and incompatible demands: for reliable authentication in one case, but for reliable protocols to be undermined in another.

Intermediary Liability Undermines Trust and Security Without Achieving Its Goal

Preventing the spread of illegal content online is an important goal, and we should all strive to find solutions. However, illegal content—and the behavior that produces it—existed long before the Internet and, at its root, is a societal problem rather than a primarily technical one.

An exclusive focus on solving the problem of illegal content by breaking encryption weakens security. It diverts effort from other options, such as improving the overall capabilities of law enforcement organizations to deal with technically-mediated crime7—whether or not encryption is involved. Furthermore, relying solely on technological fixes to societal problems can create perverse incentives and lead to unintended harm, and is seldom effective in the long run.

- Preventing confidential messaging apps from delivering confidentiality renders them pointless at best, and actively harmful at worst. The Internet is not made safer or more beneficial by such measures.
- Contradictory policies on authentication create further confusion and technical complexity, undermining users' trust in online services and confidential communication.

---

5 https://www.chinalawtranslate.com/en/provisions-on-the-management-of-internet-forum-community-services/

6 https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/

7 https://eshoo.house.gov/sites/eshoo.house.gov/files/migrated/wp-content/uploads/2019/10/Eshoo-Wyden-Letter-to-AG-Barr-re-encryption.pdf

While the Internet may sometimes be used for harm, we should resist legal proposals that require service providers to override people's ability to secure their information and interactions online. To do so places individuals and organizations at greater risk with no guarantee of achieving the intended outcome. We encourage policymakers to support strong encryption policies and practices. This will help keep people, infrastructure, and countries safe online, and maintain the Internet as a global vehicle for innovation, education, and social and economic progress.