Encryption

Encryption technologies enable Internet users to protect the integrity and the confidentiality of their data and communications. From limiting the impact of data breaches to keeping messages private, encryption is an essential tool for digital security. As a technical foundation for trust on the Internet, encryption promotes freedom of expression, commerce, privacy, and user trust, and helps protect data and communications from bad actors.

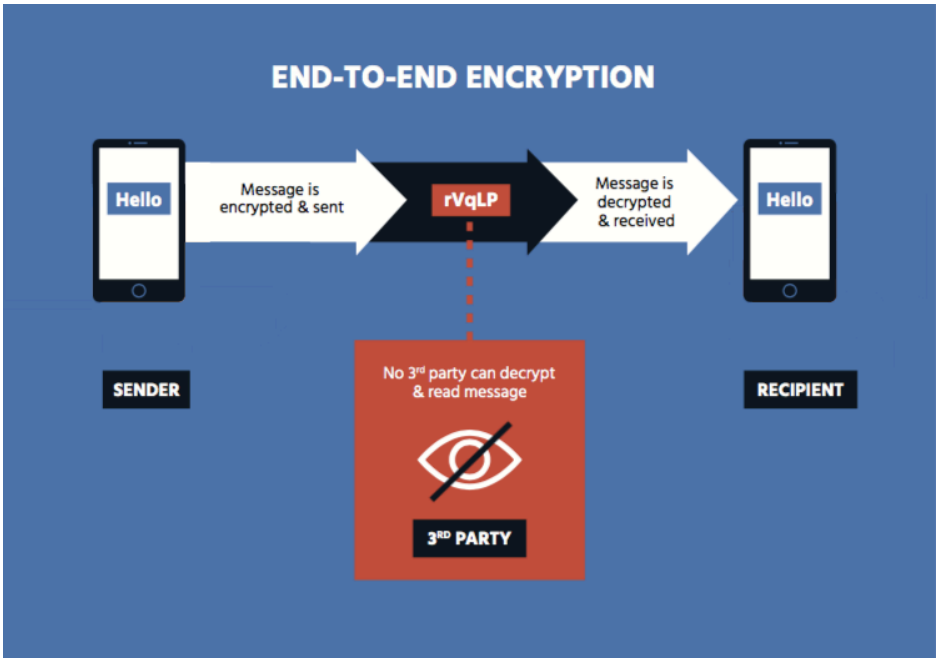
The Internet Society believes encryption should be the norm for Internet traffic and data storage.

What is encryption?

Encryption is the process of scrambling or enciphering data so it can be read only by someone with the means to return it to its original state. It is commonly used to protect both data stored on computer systems **(data-at-rest),** and data transmitted via computer networks, including the Internet **(data-in-transit).** For data-in-transit, data is generally scrambled using a public key and unscrambled using a private key. For data-at-rest, the secret value is typically known only by the data owner.

End-to-End Encryption

End-to-end (E2E) encryption is any form of encryption in which only the sender and intended reipient hold the keys to decrypt the message. The most important aspect of E2E encryption is that no third party, even the party providing the communication service, has knowledge of the encryption keys.



We rely on encryption every day

Web browsing: Browsers and websites use HTTPS, an encrypted protocol, to provide secure communications, keeping our data from being read by criminals while in transit.

E-commerce: We trust companies to protect our financial information when we buy things online or use online banking. Encryption is an important method of doing that.

Secure messaging: When we use a messaging app, we expect the messages to be private. Some messaging apps use encryption to maintain the privacy and security of their users' communications while it is in transit. Others even use end-to-end encryption, so only the sender and receiver can read the messages, e.g. iMessage, WhatsApp, and Signal.

What is Exceptional Access?

Generally, when people speak of exceptional access they refer to some means of allowing law enforcement the ability to lawfully access the content of communications and data in an unencrypted form.

Why Exceptional Access?

Because bad actors can also use encryption to hide their activities, there is concern among law enforcement and some others about the negative impact encryption could have on their ability to protect citizens and enforce the law. Some argue that law enforcment should be given exceptional access to the content of encrypted communications and devices.

Problems with Exceptional Access

No matter the method, exceptional access makes it easier for other parties, like criminals and other governments, to gain access to secured data. The consensus among information security experts is that exceptional access mechanisms always add more complexity to systems, leading to vulnerabilities. These vulnerabilities can act as points of entry that anyone could discover.

Proposals for exceptional access are unlikely to prevent criminals from freely communicating in secret. For actors with some computer experience it is fairly easy to find alternative tools to encrypt their data at rest or in motion. The communications of determined criminals could be immune from observation and everyday users' communications could be left vulnerable to observation and interception by bad actors who have discovered how to exploit the vulnerabilities created through exceptional access.

Some Exceptional Access Proposals

An encryption backdoor generally refers to some change to an encryption protocol, application or service that is intended to allow authorized third party access to encrypted data. One way to do this is by **weakening the encryption** mechanisms or the systems supporting them. Backdoors of any type are vulnerabilities that can be discovered and used by criminals and other bad actors.

Key escrow generally refers to the idea that decryption keys would be stored in the custody of a trusted third party for later use by law enforcement. But, any stored keys are at risk of being misused by criminals and other bad actors.

Luggage locks – A metaphor for encryption backdoors

TSA-approved luggage locks were designed to allow travelers to secure their luggage while at the same time providing TSA with the ability to open their luggage and inspect the contents for security purposes, by using a master key held by the TSA.

Unfortunately, the master keys did not stay secret: their design was exposed, allowing copies to be reproduced with a 3D printer or purchased online for as little as $10.

Now anyone can obtain a master key and open TSA-approved locks.

Considerations on Exceptional Access

If encryption or other security mechanisms are weakened to enable forensic access, it becomes easier for any party to gain access (particularly organized crime, corporations involved in industrial espionage and nation-state actors). It also undermines the legitimate interests of private citizens and corporations by facilitating identity theft and access to sensitive information about assets, including both financial and intellectual property.

The Internet Society recognizes the concerns of law enforcement and remains firm in its conviction that encryption is an important technical solution that all Internet users should use to protect their communications and data. Legal and technical attempts to limit the use of encryption, even if well-intentioned, will negatively impact the security of law-abiding citizens and of the Internet at large.

Exceptional access proposals do little to solve the problem of criminals communicating in-secret and they are likely to introduce substantial risk to law-abiding citizens. Exceptional access will bring new problems, without delivering an effective solution.