Encryption uses math to scramble data to protect it from prying eyes. To read encrypted data, a person must have a unique key or password to unscramble the data making it legible.

So if encryption is good for us, what’s the debate?

Some tech companies are launching products that automatically encrypt data in a way that only the user can decrypt. Silicon Valley, computer scientists, and activists argue that more encryption keeps data and people safe.

Law enforcement argues that automatically encrypting data will make the contents of a message between two suspects in a criminal investigation impossible to read.

It keeps credit card information safe when purchasing something online.

It keeps data, such as images, health data, and financial data, safe from prying eyes.

It keeps classified information secret.

It keeps credit card information safe when purchasing something online.

It keeps data, such as images, health data, and financial data, safe from prying eyes.

It keeps classified information secret.

Why does law enforcement want access to some data?

The ability to decrypt encrypted communications could enable law enforcement to:

- Obtain operational details or evidence of terrorist plots, espionage, or other criminal activity.
- Gather evidence.
- Act quickly in emergency situations, such as when someone’s life is in immediate danger.

It is impossible to create a method that only allows law enforcement to decrypt data without giving that same capability to criminals and terrorists.

Lawful hacking

Law enforcement should have the ability to hack into a suspect’s smartphone or computer with a court order using existing software vulnerabilities, instead of requiring companies to maintain a decryption capability.

Develop national capacity to decrypt data

Law enforcement should have the ability to hack into a suspect’s smartphone or computer with a court order using existing software vulnerabilities, instead of requiring companies to maintain a decryption capability.

Increase police tech literacy

Recognizing how and when encryption occurs—on the device, in transit, and in the cloud—may help law enforcement access the data it needs.

Where can law enforcement attempt to access encrypted data?

On a device

In transit

In the cloud

Everywhere

What are the arguments against requiring tech companies to maintain the ability to decrypt data for law enforcement?

- Why does encryption occur?

- So if encryption is good for us, what’s the debate?

- Why does law enforcement want access to some data?

- Where can law enforcement attempt to access encrypted data?

- What are the arguments against requiring tech companies to maintain the ability to decrypt data for law enforcement?

- What alternatives have been proposed to help law enforcement access the data they seek?

- Increase police tech literacy

- Develop national capacity to decrypt data

- Lawful hacking

- Collecting Metadata

- Internet-enabled devices contain metadata. A smartphone can contain data and information about other devices it talks to, which is called metadata. This metadata can help law enforcement investigate a suspect or an encryption online.

COFAFIR - FOREIGN RELATIONS
cfr.org/cyber