# The Benefits of Encryption

Encryption is the technology that keeps the data on our phones, tablets, and other gadgets safe from unauthorized access. End to End Encryption (e2ee) ensures the privacy and confidentiality of messages exchanged between users. Cryptographic techniques are used to scramble your data or your messages, making them unreadable to anyone other than you or the intended recipient. This means that even if a malicious third party intercepts your messages, they won't be able to decipher or access your private information.

In traditional communication methods, messages are typically encrypted during transmission, but they can be decrypted and accessed by service providers or intermediaries at various points along the communication path. However, with e2ee, the message is encrypted on the sender's device, remains encrypted while in transit, and can only be decrypted by the intended recipient's device. This means that even if someone intercepts the message during transmission or gains access to the communication service provider's servers, they cannot decipher the content.

**Encrypted Services Provide Privacy and Security**
In a world where data, including the content of messages, is frequently collected, and exploited, both by data brokers and law enforcement, encrypted messaging services provide much needed privacy. E2ee message systems are not able to store or analyze conversations, ensuring that personal information remains confidential and out of the reach of corporations, advertisers, or government surveillance.

**“Exceptional Access” for Law Enforcement Is “Open Access” for Other Bad Actors**
Encryption is a critical first step to preserving the safety and privacy for all people, including children, seniors, journalists, foreign services officers and their families, active-duty service members and their families, and anyone who wants to be able have a private conversation without government surveillance.

Law enforcement asserts that encryption prevents them from doing their jobs. However, while e2ee secures the content of messages, it doesn't protect metadata, such as the sender, recipient, or timestamps, which can still be visible to service providers and law enforcement.

Additionally, there is no technological compromise between strong encryption that protects the data and a mechanism to allow the government “exceptional access” to this data. Building an exceptional access mechanism on the vast scale needed to decrypt messages on a routine basis would put everyone at greater risk of hacking, identity theft, and fraud. In addition, any system implemented by the US government *will* be accessed and misused by repressive governments around the world, including against Americans.

**Want more information?** Please contact Director of Federal Affairs India McKinney at india@eff.org.

EFF

The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation.
Learn More: https://www.eff.org/issues/security