# Encryption

## How It Can Protect Journalists and the Free Press

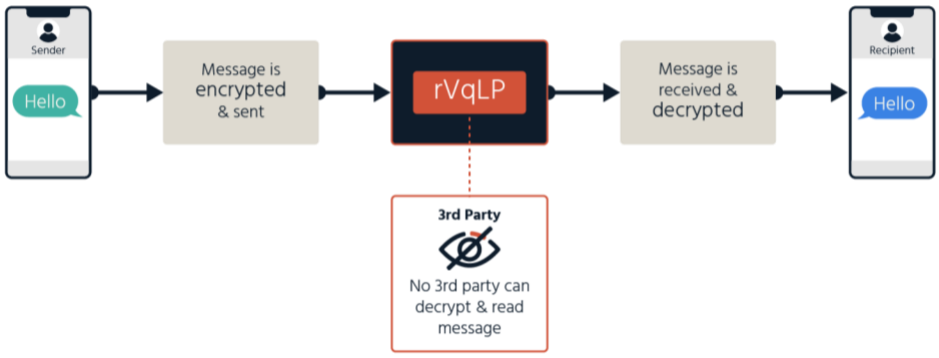
August 2022

Encryption is a tool designed to help Internet users keep their online data and communications private and secure. It plays a critical role in protecting day-to-day digital activities like online banking, shopping, preventing theft of sensitive information in data breaches, and making sure private messages stay private.

Encryption is essential for protecting freedom of expression and privacy.

**What is encryption?**

Encryption is the process of scrambling information so it can only be read by someone with the keys to open and unscramble the information. End-to-End (E2E) encryption provides the strongest level of security and trust, because by design only the intended recipient holds the key to decrypt the message. No third party should have a key.




For some communities, like journalists, encryption is especially crucial for keeping people safe and ensuring a healthy freedom of the press.

## Encryption and Journalists' Safety

Encryption is an essential tool for journalists. If journalists cannot communicate in confidence with colleagues and sources, they cannot do their jobs in safety. Likewise, if they cannot protect the anonymity of their sources, those sources may not come forward, and the public will pay the price.

**Safely connecting with sources**: Journalists' sources sometimes share incriminating information about an institution or personal information about themselves only if journalists agree to protect their identity. End- to-end encryption allows journalists to build a trusted relationship with these sources.

**Protecting the integrity of information**: Journalists need to reliably signal to readers that they have created trustworthy content and ensure it matches what their intended audience can see online.

Internet protocols like HTTPS help protect data as it passes between news websites and reader. It also protects journalism from censorship: it's harder for censors to block messages or access to news if they cannot intercept the content.

**Protection from attackers**: There are many cases of journalists and news outlets having their devices and online platforms hacked and surveilled by government and private actors over their reporting, including one case in which the US National Security Agency (NSA) reportedly hacked into Al-Jazeera's internal communication system. Journalists also face threats such as online abuse, doxxing (gathering and publishing personal information online), and stalking. End-to-end encryption helps protect their communications from surveillance and interception by third parties.

**Holding governments and institutions accountable**: An important component of journalism is its ability to hold people and institutions in power accountable for their decisions and actions. To do this, it is critical for journalists to have digital security tools that prevents powerful entities—domestic or foreign—from accessing and/or altering their research, conversations, and sources.

**Strong encryption policy protects journalists everywhere**: When countries support end- to-end encryption, they help journalists in their own nations and around the world by setting a standard for global encryption protections.

Encryption enabled journalists to expose global corruption

The Panama Papers leak began in late 2014 when an unknown source reached out to Bastian Obermayer, a reporter for the German newspaper Suddeutsche Zeitung. Obermayer says the source contacted him via encrypted chat and offered data intended "to make these crimes public." But the source warned that his or her "life is in danger," was only willing to communicate via encrypted channels, and refused to meet in person. The Panama Papers leak revealed a Panamanian law firm's global tax evasion system for its clients. It comprised 2.6 terabytes of data—11.5 million documents—and involved around 400 journalists from more than 100 media organizations in over 80 countries working together to tell the stories hidden within.

Encryption helped whistleblower connect with journalists

In 2015, The Intercept received files from an individual through SecureDrop, software designed to help whistleblowers anonymously leak information to the media. The story showed that Securus, a company that provides phone services to more than 2,200 prisons in the U.S., kept records of every phone call made by the more than 1.2 million inmates who use the service in 37 states—including the time, phone numbers called, inmate names, and even the audio recordings of every call. The records were routinely sold to law enforcement customers, including inmate conversations with lawyers meant to be protected by attorney-client privilege. The shocking revelation only surfaced because an individual who accessed the files shared them with The Intercept via SecureDrop.

## Why "Exceptional Access" Isn't the Answer

"Exceptional access" generally refers to giving law enforcement and intelligence agencies the power to either intercept and access encrypted communications or compel companies to do it for them. This not only weakens security on the Internet; it also puts journalists at risk both online and in real life. Here's how:

- **Forced weakness weakens us all**: Any point of entry to a secure service is a weakness. Exceptional access puts private information and conversations at risk because it allows government access to your private information, and simultaneously creates a doorway for bad actors. There is no digital lock that only the "good guys" can open and others cannot.
- **Lack of encryption can deter journalists from publishing risky content**: If journalists do not have a secure way of performing their work, they may opt to not pursue sensitive stories due to potential backlash, scrutiny, and harassment they may receive. A healthy democratic nation needs a strong and independent free press to inform the public about the actions of governments, institutions, and companies it chooses to trust.

## Recommendation

Protect freedom of the press by advocating for strong end-to-end encryption and ensuring journalists and the public are free to use it. Journalists need to be safe online in order to hold governments and institutions accountable, tell important and impactful stories, protect their sources, and promote healthy democracies.

## Learn More About How Encryption Affects Journalists

For more information, go to www.cpj.org and @pressfreedom on Twitter.

## Internet Society Encryption Resources and Training

https://www.internetsociety.org/issues/encryption/resources/

https://www.internetsociety.org/learning/encryption/