Encryption

How It Can Protect Advocacy Groups and Social Change Movements

October 2021

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.

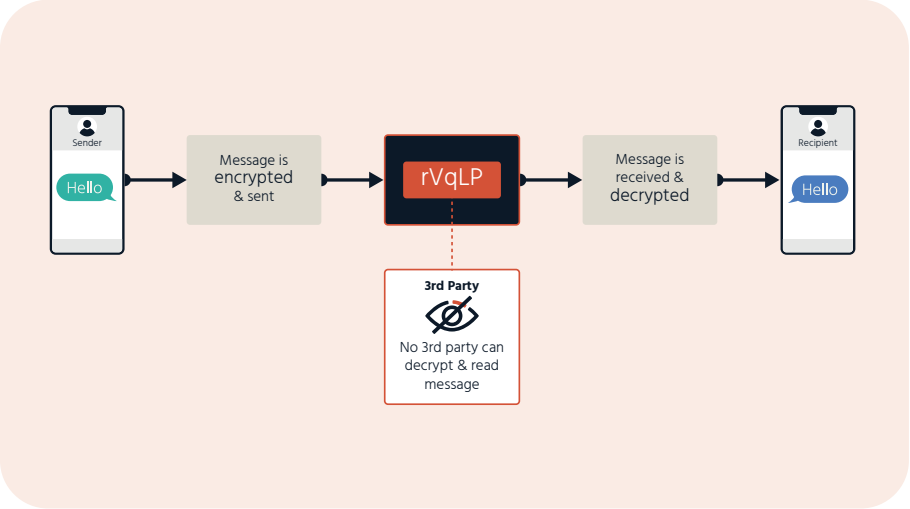
It is essential for protecting freedom of expression and privacy. For some communities, like human rights defenders, advocacy groups, community organizers, and humanitarian actors, encryption is especially crucial and should be used with other more conventional privacy protection tools to keep people safe both online and in their everyday lives.

How Encryption Supports the Safety of Advocacy Groups

Encryption is an essential tool that enables advocacy groups to raise public awareness on instances of human rights violations and to hold governments to account. If advocacy groups cannot share resources and engage stakeholders in confidence, they cannot defend human rights in safety. Likewise, if advocacy groups cannot protect the anonymity of their community supporters, these supporters may not come forward, to the detriment of the public as human rights continue to deteriorate. Here are a few of the ways in which advocacy groups rely on encryption:

- Safely engage with community stakeholders: Members of the community including journalists, interest groups, academics, and individuals will share resources and personal information about themselves only if advocacy groups agree to protect their identity. End-to-end encryption allows advocacy groups to build a trusted relationship with their community, growing their movement while minimizing the risk to individuals.
- Protecting the integrity of information: Advocacy groups need to reliably signal to the community that they have shared trustworthy information. Internet protocols like HTTPS help protect data as it passes between websites and readers. It also protects advocacy groups from censorship: it's harder for censors to block messages or access to websites if they cannot intercept the content.
- Protection from personal attack: There are many cases of advocacy groups having their devices and online platforms hacked and surveilled by government and private actors, including one case in which NSO Group's spyware was used to surveil over 50,000 targets including heads of state, activists and journalists, as revealed by the Pegasus Project. Advocacy groups also face threats such as online abuse, doxxing (gathering and publishing personal information online), stalking, and in extreme cases, kidnapping and violence. While advocacy groups must remain alert to a myriad of surveillance techniques, both digital and more traditional, end-to-end encryption helps increase protection for their communications from surveillance and interception by third parties. While hacking and surveillance can still happen on user devices, weakening encryption services, or not using them at all, would make such attacks even easier and more common.
- Holding governments and institutions accountable: An important part of human rights advocacy is being able to hold people and institutions in power accountable for their decisions and actions. To do this, it is critical for advocacy groups to have digital security tools that prevents powerful entities—domestic or foreign—from accessing and/or altering their research, conversations, and community databases.
- Strong encryption policy protects advocacy groups everywhere: When countries support end-to-end encryption, they help both local and international advocacy groups by setting a standard for global encryption protections. When countries weaken encryption, they set a dangerous precedent that could be abused by foreign governments that lack the same robust rule-of-law standards.

Internet Society



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 access to that key. But some governments and organizations are pushing to weaken encryption as a means to fight crime.

Why Encryption Backdoors Aren't the Answer

Law enforcement and intelligence agencies are increasingly asking for "Encryption backdoors" to intercept or access encrypted communications to help 'catch the bad guys' themselves, or order companies to do it for them. This not only weakens the global Internet infrastructure; it also puts the lives of human rights defenders at greater risk of harm. Here's how:

- Forced weakness weakens us all: Any point of entry to a secure service is a weakness. Encryption backdoors puts private information and conversations at risk because it allows government access to your private information, but simultaneously creates a doorway for bad actors through the same entry point. There is no digital lock that only the "good guys" can open and others cannot.
- Criminality is subjective: While authorities may argue that encryption backdoors can help catch criminals, in far too many countries insufficient rule-of-law standards result in genuine human rights defenders being prosecuted and harassed by authorities. Advocacy groups and humanitarian actors in some countries can be subject to prison, torture and even the death penalty for drawing attention to human rights abuses
- and exercising their freedom of expression. Without encryption, advocates living in or traveling to these countries may not be able to safely and comfortably advocate for victims of abuse and would be left vulnerable to prosecution and persecution.
- Lack of encryption can erode the mechanisms for holding power to account: If advocacy groups do not have a secure way of performing their work, they may opt to not pursue high profile issues due to the potential backlash, scrutiny, and harassment they may receive. A healthy democratic nation needs a strong and vocal community to bring attention to the societal impact of the actions of governments, institutions, companies, and other powerful actors.

Protect Encryption, Protect Yourself

Protect our strongest digital tools to keep people safe online. Both advocacy groups and the public need to be safe online in order to hold governments and institutions accountable, tell important and impactful stories, and promote healthy democracies.

- Use end-to-end encrypted communications services.
- Learn more about how encryption works, why it's under threat and how you can protect yourself.
- Take the Internet Society's free online Encryption training course.
- Join the Friends of the Global Encryption Coalition to keep up to date with the latest encryption news around the world.
- Join your local Internet Society Chapter to advocate for encryption in your country or region.

Internet Society