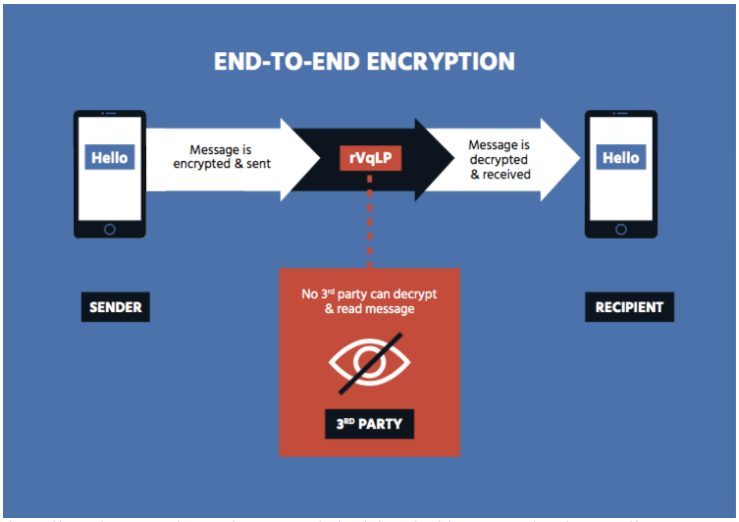
Encryption

Essential for the LGBTQ+ Community

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

Encryption is essential in establishing a foundation of trust online that helps protect freedom of expression and privacy. For some communities, like LGBTQ+ communities, encryption is especially crucial in keeping people safe both online and in real life.



https://www.internetsociety.org/wp-content/uploads/2018/06/Short-encryption-doc_EN.pdf

The Internet is an essential tool that helps the LGBTQ+ community live their truth without fear of persecution while protecting their privacy; **strong encryption** is a critical part of that equation.

Encryption and LGBTQ+ Communities

Encryption plays a vital role in the safety and well-being of LGBTQ+ communities:

Privacy While Coming Out and Connecting: Coming out safely and finding a trusted community to connect with can be difficult. LGBTQ+ people may risk losing family and friends by coming out, so they often rely on online communities to find support systems. Our research shows that LGBT people are core users of the Internet with 80% of LGBT people saying that they participate in a social networking site compared to 58% of the general public. Encryption can be a potent tool that empowers people to use the Internet to venture out of the closet in a safe way. For many teens, who may still live at home with non-supportive family members, encryption may be the only tool allowing them to come out safely and on their terms.

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 ideally only the intended recipient holds the key to decrypt the message. No third party should have a key.

Trans Communities: Transgender communities have unique challenges and are especially vulnerable to violence, unemployment, and persecution. The Internet affords transgender communities opportunities to build a support network of other transgender people and allies. Encryption can help ensure online communications and activities are kept private, minimizing the risk of violence and stigma that disproportionately affects this community.

Access to Healthcare: Encryption is a tool that can empower transgender people to safely use the Internet to find doctors and treatment during transitions. Doctors will often use end-to-end encrypted services to care for

transgender patients safely and securely without the risk of their sensitive health data being compromised. Encryption also allows LGBTQ+ individuals to communicate with accepting and trusted healthcare providers in an open and candid manner thereby greatly increasing the quality of health service and health outcomes (for example, our research found that up to 45% of lesbian and bisexual women are not out to their doctor).

Protecting Against Discrimination: In the U.S., it is still legal for LGBTQ+ people to face discrimination in housing, employment, and many other sectors for being who they are. For instance, only 22 states and the District of Columbia prohibit employment discrimination on the basis of sexual orientation or gender identity; this means there are 28 states where companies can fire their employees for identifying as LGBTQ+. With encryption, members of these communities are better equipped to protect their privacy and choose whether or not to share their identification with others.

Strong Encryption in the U.S. Protects LGBTQ+ Communities Everywhere: As is true for many technologies with headquarters based in the U.S., policy decisions made here will affect and set precedents around the world. If the United States plays a leadership role in creating policies that support strong encryption, it may be easier to persuade other countries to follow suit.

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 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 LGBTQ+ communities at greater risk of harm. 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, 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; In far too many countries, LGBTQ+ are still considered criminals: While authorities may argue that exceptional access can help catch criminals, in many countries (between 72 and 76 at last count) being LGBTQ+ is considered a criminal offense. LGBTQ+ people in these countries are subject to prison, torture and even the death penalty simply for expressing their identity. In numerous additional countries, 'gay propaganda' or the act of speaking out about LGBTQ+ issues on its own is a criminal activity. Without encryption, LGBTQ+ individuals living in or traveling to these countries may not be able to safely and comfortably find communities and outlets for self-expression and would be left vulnerable to prosecution and persecution.

Recommendation:

Protect our strongest digital tools to keep people safe online. Strong encryption **helps ensure the safety, privacy, and livelihoods of LGBTQ+ and other vulnerable communities around the world.**

Sources:
https://www.hrc.org/state-maps/employment
https://www.nytimes.com/2019/10/08/us/politics/supreme-court-gay-transgender.html
https://www.cbc.ca/news/technology/usa-border-phones-search-1.4494371
https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html
https://www.internetsociety.org/wp-content/uploads/2018/06/Short-encryption-doc_EN.pdf
https://docs.wixstatic.com/ugd/699ad7_b0219ea9c8804c05a03d95ca7f911f78.pdf