https://www.apc.org/en/news/what-encryption-and-why-it-key-human-rights

What is encryption and why is it key to human rights?

By Verónica Ferrari* -- 24-04-2024

What is encryption?

Encryption is the process of making messages or files unreadable by anyone except for people who have the key or password to decrypt them. During encryption, a file is encoded in a way that converts the original representation into an alternative form that can only be deciphered (converted back) by authorised parties following a certain procedure and using a key or password. As APC member Open Net Korea says, it is saying something "in a secret language that is known only to a closed group of people."

Encryption is one of the best techniques that we have to protect information from interference when navigating the internet and in our devices and email. Encryption can be implemented using software applications, special hardware or a combination of both. A stronger form of encryption is end-to-end encryption, which encrypts data even before it is sent to a server. When used correctly, it is virtually impossible (or extremely time consuming) to break with current technologies.

Why is encryption key to human rights?

Encryption is key to preserving confidentiality and anonymity in our online communications, and is therefore essential for the enjoyment of a range of human rights. In its latest resolution on privacy in the digital age, the UN Human Rights Council stressed the importance of encryption, pseudonymisation and anonymity to ensure, in particular, the enjoyment of the rights to privacy, to freedom of opinion and expression, and to freedom of peaceful assembly and association.

In June 2015, the UN Special Rapporteur on freedom of opinion and expression dedicated a report to the fundamental role of encryption for the full exercise of the right to freedom of expression, and examined the ways in which encryption establishes, among other things, a measure of privacy that enables people to use the internet to develop opinions and access information online without interference. The report also explores how anonymity is linked to the right to privacy and explains that "an individual cannot have a reasonable expectation that his or her privacy is being protected without the ability to control what information is shared about them and how that information is used."

As APC has emphasised, anonymity is also inextricably linked to the right to privacy. And the lack of privacy, or even the perception of the lack of privacy, can have a chilling effect on freedom of expression and lead to self-censorship.

The mandate of the United Nations Special Rapporteur on freedom of peaceful assembly and association has also addressed the importance of encryption

providing a safe online space to gather, connect, organise and coordinate activities, without undue interference from third parties and governments.

Encryption is also connected with self-determination and the ways in which we occupy digital spaces. APC member May First Movement Technology considers encryption to be a key part of "the struggle to regain democratic and community ownership of our data and technology infrastructure and development itself."

As we stated in our explainer on cybersecurity, weakened encryption undermines human rights: it can make it easier for malicious actors to gain access to people's personal information and communications, can lead to journalists' sources being revealed, human rights defenders being targeted by governments, and a person in an abusive relationship being blackmailed. Encryption and anonymity provide the privacy and security necessary for the exercise of a range of rights and should be strengthened.

Why does encryption especially matter for women and people of diverse gender and sexual expressions?

Women and people of diverse gender and sexual expressions are especially vulnerable to violations of privacy, since their experiences take place within a context of existing structural inequalities and discrimination that put them at particular risk of violence and other types of human rights violations. Therefore, encryption and anonymity are essential tools to empower and protect groups at risk, specifically sexual and gender rights activists and those who are targets of online violence.

The United Nations High Commissioner for Human Rights noted in a report from 2017 that women's right to privacy implies the ability to benefit from encryption and anonymity "in order to minimize the risk of interference with privacy, which is especially pertinent for women human rights defenders and women trying to obtain information otherwise considered taboo in their societies." In her soon to be officially launched new report on gender justice and freedom of expression, Irene Kahn, the UN Special Rapporteur on freedom of expression, states that anonymity and encryption "are an essential facet of women's enjoyment of freedom of opinion and expression in the online context and must be protected."

Anonymity is an important enabler of the right to be free from discrimination, since it enables individuals and minority groups, among others, to associate on sensitive matters such as sexual orientation. Anonymity and encryption are also tools to combat hate speech and online violence and to empower the expression and realisation of sexual rights, as APC has stressed.

It is also important to note that the use of encryption is not only essential to protect human rights online, but also offline, due to the continuum between the online and offline spheres. Groups at risk face consequences that are not solely related to their online interactions and communications, but also have implications for their lived realities. Restrictions to encryption can endanger the physical integrity and life of specific groups at risk.

Finally, APC's Feminist Principles of the Internet explain that anonymity on the internet enables freedom of expression online, particularly when it comes to breaking taboos of sexuality and heteronormativity and experimenting with gender identity, and provides a safe space for women and queer persons affected by discrimination.

What should states and companies do about it?

Many states (and companies) have implemented or proposed measures to weaken encryption tools. For example, through the inclusion of "backdoors" in products, they can bypass the strongest protection and have unlimited access to seemingly secured information. The so-called backdoors can lead to journalists' sources being revealed, human rights defenders and their networks being targeted, or a person in an abusive relationship being blackmailed. As former UN Special Rapporteur on freedom of expression David Kaye said in his report of 2015: "Requiring encryption back-door access, even if for legitimate purposes, threatens the privacy necessary to the unencumbered exercise of the right to freedom of expression."

Countries around the world have also put in place legal bans on the use of encryption of communications, in the name of security and law enforcement. Research by APC member CIPESA found that in Africa, many countries have passed legislation that limits anonymity and the use of encryption through criminalisation of possession and use of cryptographic software or hardware. These trends are accompanied by an increasing persecution of digital security researchers and technical experts who identify and report on vulnerabilities in digital systems to benefit the public at large, such as the case of Ola Bini in Ecuador.

As the UN Special Rapporteur on freedom of expression recommended, states should promote strong encryption and anonymity and should refrain from these measures that interfere with the use of such technologies. Additionally, as APC has said in the past, states should also put in place effective mechanisms for remedy that protect individuals whose rights have been violated due to limitations on anonymity, particularly for individuals from groups at risk.

Companies developing digital services and products have the responsibility to respect human rights, as established by the UN Guiding Principles on Business and Human Rights. Therefore, businesses as well as states should refrain from blocking or limiting the transmission of encrypted communications and, as the UN Human Rights Council stressed, work towards enabling encryption technologies.

In the words of Natasha Msonza, co-founder and chief operations officer of the Digital Society of Africa (DSA) and an APC individual member, "governments and companies should in fact especially be actively promoting and using encryption themselves," as there are malicious actors after their data, too.

Make the switch: Global Encryption Day

Encryption and anonymity-enhancing technologies are essential for the full realisation of the right to privacy, to be free from discrimination, and for the exercise of the freedoms of expression and of association and assembly, among other rights. Proposals for backdoor access, laws that criminalise the use of these tools, and the persecution of digital security experts, among other measures, pose threats to these rights.

Join APC in our activities around the first annual Global Encryption Day this 21 October.

This date will mark an opportunity to tell governments and companies around the world about the right of people to use encryption to ensure secure, private and anonymous online communications, to stress to them that protecting and strengthening encryption is crucial for human rights, and to call on them to act on their commitments and responsibilities in this context.

(*) Contributions to this article were also made by Roxana Bassi, APC's tech coordinator, and Valeria Betancourt, manager of the APC Communications and Information Policy Programme.

Find some highlights from this article ready to share on social media here.
#GlobalEncryptionDay #MakeTheSwitch