Innocenti Research Brief

2020-30

unicef
Office of Research-Innocenti

# What is encryption and why does it matter for children?

## Summary Note by UNICEF's Cross-divisional Working Group on Child Online Protection

Encryption encodes information so that it can only be read by certain people. 'End-to-end' is a robust form of encryption where only the users communicating can read the information. In other words, third parties – such as service providers – cannot decrypt the information.

It matters for children because while it protects their data and right to privacy and freedom of expression, it also impedes efforts to monitor and remove child sexual abuse materials and to identify offenders attempting to exploit children online.

### HOW DOES END-TO-END ENCRYPTION WORK?

It scrambles communication so that it cannot be read by anyone unless they have the corresponding key. In end-to-end encryption, third party intermediaries do not have keys to decrypt the communication; it is only readable by the parties exchanging information.

All IT-systems use a level of encryption to be secure. Corporations and states use it to protect against threats to national security such as cyber warfare, data breaches and interference with elections. Encryption is fundamental for states to protect their citizens, including children.

### WHY IS END-TO-END ENCRYPTION IMPORTANT?

In some countries, it protects people – especially the most vulnerable and marginalized – from serious risks of human rights violations and persecution. In 2019, Freedom House reported that of the world's 3.8 billion people with internet access:

- **71 per cent** live in countries where people were arrested or imprisoned for posting content on political, social or religious issues.
- **65 per cent** live in countries where people have been attacked or killed for their online activities.

End-to-end encryption means that every person, child or adult, is provided with a digital shield against potential violations of their right to privacy and freedom of expression.

Encryption is also critical to children's safety. Children's digital communications contain personal information. If that were to fall into the wrong hands, it could jeopardize both their privacy and safety.

### HOW DOES THIS IMPEDE EFFORTS TO TACKLE CHILD SEXUAL EXPLOITATION AND ABUSE?

If law enforcement cannot read encrypted communications, it is more difficult for them to prevent sexual abuse images from being shared online. With each share or view, the child is re-victimized. Implementation of end-to-end encryption on digital communications platforms also significantly reduces the number of reports made by watchdog organizations and law enforcement. This threatens efforts for (1) increased investment in tackling child sexual exploitation and abuse; and (2) greater action taken by the technology and telecommunication industries to make their platforms safe.

### WHERE DOES THE DEBATE NOW STAND?

What appears to be a conflict, between a child's right to privacy and right to protection from sexual abuse and exploitation, will require a careful and nuanced approach. Taking an extreme or polarized position will stand in the way of thoughtful policy responses. To ensure that children's rights are safeguarded in the digital age involves fulfillment of their rights to both privacy and protection from sexual abuse and exploitation.

### WHAT ARE SOME PROPOSED SOLUTIONS?

Solutions – both technological and legal – have been put forward, each with pros and cons that need careful consideration.

### Granting exceptional access to law enforcement

Some actors, including governments, have proposed that technology platforms should provide exceptional access ('backdoors') for law enforcement to access and seize personal information through a search warrant.

**Pros:** Allows law enforcement to operate more effectively in a digital environment.

**Cons:** Makes the system vulnerable to unauthorized access by (malicious) third parties, even if intended solely for use by law enforcement. Governments themselves may also abuse this power. Once in place, there is a risk that the boundaries for when these can be used could shift over time and come to include a greater number of offenses (some of which are not illegal).

### Running outgoing images through a 'filter'

This is called 'client-side scanning' and means that outgoing communication from a personal device is checked against a list of known child sexual abuse images. If there is a match, the system refuses to send the message or reports it to law enforcement or watchdog organizations.

**Pros:** This solution is more data protection-friendly compared to exceptional access because it does not create a vulnerability in the system.

**Cons**: Any 'filter' presents a potential threat to the freedom of expression. Also, unless the list is open to the public, it risks providing a blueprint for mass surveillance. Other sensitive but legal content (such as political or sexual) could be added to the list without the user's knowledge.

### 'Compelled disclosure'

This authorizes law enforcement to force a suspect to either hand over the key to the encrypted system or to provide them with plain text data from their device.

**Pros:** Police can target suspects and retrieve the information they require without a general vulnerability being created within the encrypted system.

**Cons:** It is reactive rather than proactive. Also, it requires a suspect and legal process before the illegal materials can be found, which would still impede the use of tools that can remove child sexual abuse materials systematically.

## KEY TAKEAWAYS

1. Without a nuanced position on encryption, there is a risk of inadvertently supporting the dilution of the rule of law and compromising children's safety. Technological and legal solutions must be weighed carefully to ensure that all of children's rights are respected.

2. Greater investment – in time, resources and consultation with experts – is required to develop an evidence-based, nuanced position.

3. A popular but incorrect claim in the debate is that: Children will have their rights better respected if digital communications platforms remain unencrypted. Child rights advocates should neither push for the unlimited use of end-to-end encryption, nor for its complete abolishment. These extreme positions do not serve children's best interests.

4. It is important to communicate that children's safety in a digital age encompasses not only protection from sexual exploitation and abuse, but also ensuring privacy and security. This is reflected in UNICEF's newly proposed Child Online Protection strategy. UNICEF and others should advocate with industry partners to increase efforts to develop technical solutions that safeguard both of these rights.

---

This note summarizes a more comprehensive brief produced by UNICEF's Cross-Divisional Working Group on Child Online Protection on the challenges and opportunities related to the use of end-to-end encryption technology.



**UNICEF OFFICE OF RESEARCH-INNOCENTI**
Florence, Italy

www.unicef-irc.org

+39 055 20330

florence@unicef.org
@UNICEFInnocenti
facebook.com/UnicefInnocenti

**For every child, answers**