National Center for Missing and Exploited Children

Children's Rights

https://www.missingkids.org/theissues/end-to-end-encryption

Campaign and Advocacy

Get the latest updates from NCMEC

End-to-end encryption is a term used to describe blocking or preventing any third-party recipient from viewing, reading or becoming aware of information that one individual has sent to another. In response to growing concerns about online data security, many technology companies are adopting this strategy with potentially dire circumstances.

The use of end-to-end encryption would prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children.

We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.

Read NCMECs full statement on this issue here.

On February 20, 2020, NCMEC released an open letter to the technology industry outlining five *Principles to Safeguard Children in End-to-End Encrypted Environments.*

- Do not implement end-to-end encrypted communications for accounts where a user has indicated they are under 18 years old.

- Implement detection technologies, at least as effective or better than those currently available, to prevent offenders from distributing child sexual abuse material.

- Adopt technology vetted by the child protection community to identify sexual grooming of children by adults.

- Promptly report apparent child sexual exploitation to NCMECs CyberTipline with actionable information to help rescue child victims and hold offenders accountable.

- Ensure that law enforcement can use existing legal process to effectively investigatethe sexual exploitation of children.

You can view and download the entire letter here.

With no technological exception to end-to-end encryption, the dehumanizing abuse of children will continue undetected and left as collateral damage. Their abusers and the people who trade the images and videos of this abuse will be protected.

The effects are long lasting for these victims, leaving them struggling in their recovery. Survivors have spoken about their feelings of revictimization as the images and videos continue to be circulated online.

NCMEC has received over

82 million

reports of child sexual exploitation to our CyberTipline.

Children of all ages

are seen in child sexual abuse material including very young children and infants.

NCMEC estimates that
more than half

of its CyberTipline reports will vanish with end-to-end encryption, leaving abuse undetected.

We oppose privacy measures that fail to address how the internet is used to entice children into sexually exploitive situations and to traffic images and videos of children being raped and sexually abused. NCMEC calls on our tech partners to find technological solutions that will enhance consumer privacy while prioritizing child safety.

NCMEC is also working closely with our Congressional leaders, and academic and policy experts on possible legislative solutions.

Apples expanded protection for children is a game changer, said John Clark, president and CEO of NCMEC. With so many people using Apple products, these new safety measures have lifesaving potential for children who are being enticed online and whose horrific images

are being circulated in child sexual abuse material. At the National Center for Missing & Exploited Children we know this crime can only be combated if weare steadfast in our dedication to protecting children. We can only do this because technology partners, like Apple, step up and make their dedication known. The reality is that privacy and child protection can co-exist. We applaud Apple and look forward to working together to make this world a safer place for children.

NCMEC will continue to operate the CyberTipline, which was created in 1998 as a centralized reporting mechanism for suspected child sexual exploitation. Access to this information is sometimes the only way that law enforcement can rescue a child from an abusive situation and identify and arrest an offender. NCMEC staff review each tip and work to find a potential location for the incident reported so that it may be made available to the appropriate law-enforcement agency.

To make a report, visit https://report.cybertip.org/.

NCMEC will stand with survivors who are opposed to the implementation of end-to-end encryption without an exception for detecting child sexual abuse material. Many survivors fear that this would remove their only hope for the removal of the images of their abuse from online.

NCMEC will continue to work with survivors to help remove the images from online when possible.

NCMEC also provides information for survivors who want to take quick action if they are made aware of their images or videos online. Learn how to contact the internet service providers to report files circulating online.

Download theMedia Kitfor videos, graphics, and more.

This Web site is funded, in part, through a grant from the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Neither the U.S. Department of Justice nor any of its components operate, control, are responsible for, or necessarily endorse, this Web site (including, without limitation, its content, technical infrastructure, and policies, and any services or tools provided).

3.2.21.P