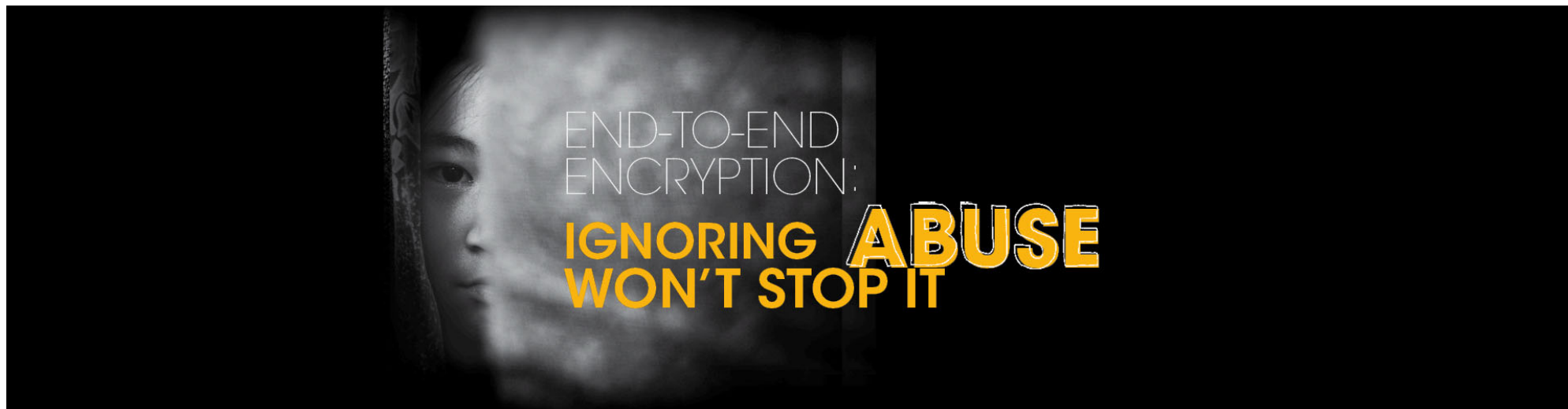


Be a champion for kids. Donate now!

End-To-End Encryption



Overview

Risk Factors

By the Numbers

What NCMEC is Doing About it

Overview

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.



We already know that social media is used to groom, lure, abuse and exploit children. Implementing available technology that would allow industry to continue to work side by side with agencies like NCMEC and law enforcement while still being able to provide end-to-end encryption and privacy to users who are not committing criminal acts shouldn't even be a question.

Children's lives and futures are in your hands.

– Survivor

Risk Factors

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.

“
It hurts me to know someone is looking at them – at me – when I was just a little girl being abused for the camera. I did not choose to be there, but now I am there forever in pictures that people are using to do sick things. I want it all erased.

– Survivor

01:52

By the Numbers

NCMEC has received more than

197 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.

What NCMEC is Doing About it

Asking Tech Companies for New Solutions

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.



As a survivor of child sexual abuse imagery I still use social media every single day. As someone who has already entrusted the tech industry with so much I trust that you will work with child protection agencies to ensure that end-to-end encryption does not create a safe haven for pedophiles. I plead, as someone who has felt the pain and deals with the lifelong repercussions of this horrendous crime, that you not extinguish what little light we have on the horizon.

– Survivor

Operating the CyberTipline

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/>.

Supporting Survivors

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.

24-Hour Call Center: 1-800-843-5678

[Blog](#)
[Careers](#)

[Media](#)
[About Us](#)

[Contact](#)
[Our Impact](#)

[Privacy Policy](#)
[Florida](#)

[Donor Privacy](#)
[New York](#)

[T&C](#)
[Texas](#)

Copyright © 2026 National Center for Missing & Exploited Children. All rights reserved.

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).