National Center for Missing and Exploited Children

Children's Rights

https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption

Public Facing Advocacy Writing

Get Updates From NCMEC

The current international discussion about privacy on the internet appropriately highlights concerns regarding online data security. We all want tech companies to ensure that our online activity isnt hacked, inadvertently disclosed to the public, or sold without our consent. But a privacy solution must be balanced with the reality that many members of the public use the internet for illegal and abusive conduct.

As the nations clearinghouse for missing and exploited children issues, the National Center for Missing & Exploited Children (NCMEC) bears witness every day to how the internet is used to perpetuate online demand for graphic sexual abuse images of children. While the sexual exploitation of a child most often occurs in private settings, abusive images and videos are shared on the most public of forums the open internet. Offenders email images to others; upload them to photo-sharing and social media sites; and share them via private chat and messenger apps. If tech companies shutter their visibility to this dehumanizing abuse of children by adopting end-to-end encryption without a solution in place to safeguard children, those who are sexually exploited will be invisible and left as collateral damage while offenders will continue to create, share, and collect child sexual abuse images without detection.

The risk to children isnt theoretical or minor. Every day at NCMEC we analyze tens of thousands of reports of children who are raped and sexually abused while photos and videos are made. Over the past 20 years, weve received more than 55 million reports of child sexual abuse to our CyberTipline - in 2018 alone we received over 18 million reports. The abuse is graphic and violent, and the sharing of images online drives the market for offenders to create more images and abuse hundreds of thousands of children each year. Many of these children are infants too young to cry out for help or identify their abusers. Many are abused by adults they trust a parent, relative or babysitter. Many are enticed and blackmailed into producing sexually explicit imagery.

Tech companies use hashing, PhotoDNA, artificial intelligence, and other technology to recognize online child sexual abuse, remove it, and report it to NCMEC. We make these reports available to law enforcement agencies around the globe. The ability for tech companies to see online abuse and report it is often the only way that law enforcement can rescue a child from an abusive situation and identify and arrest an offender.

If end-to-end encryption is implemented without a solution in place to safeguard children, NCMEC estimates that more than half of its CyberTipline reports will vanish. The transmission of child sexual abuse images and sexual enticement messages wont stop because this criminal activity is encrypted. End-to-end encryption will simply close a curtain to what happens online, enabling encrypted platforms to become lawless environments where the lack of oversight and visibility into criminal activity emboldens offenders.

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, political leaders, and academic and policy experts to come together to find technological solutions that will enhance consumer privacy while prioritizing child safety.

For more information about this issue and what NCMEC is doing about it, visit www.missingkids.org/e2ee.

Topics in this article

Online Exploitation

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).