End-to-end encryption trends and challenges - position statement

End-to-end encryption

End-to-end encryption (E2EE) is a method of secure communication that allows only the people communicating with each other to read the messages, images or files being exchanged.
Popular examples of interactive services that use E2EE are WhatsApp, Signal, Skype and Telegram — all cross-platform messaging and VoIP voice call services.

Background

Encryption is not new and, in its modern form, has been used for more than 40 years as an essential tool for privacy and security. It is primarily employed to keep data and transactions secure and to prevent data breaches and hacking. It allows legitimate, positive and safe communication where this may not otherwise be possible and is used to protect valuable information such as passport credentials.

While encryption has some positive uses, there are significant risks:

- Encryption can assist in serious harms by hiding or exacerbating criminal activities, including online child sexual abuse. Technologies that detect illegal material by proactively scanning, monitoring and filtering user content currently do not work on systems that use E2EE. Because of this, E2EE can facilitate the production, exchange and proliferation of child sexual abuse material, perpetuating the abuse of victims and exposing survivors to ongoing trauma.
- A drift towards E2EE by major social media platforms will make investigations into serious online child sexual abuse significantly more difficult. It will create digital hiding places and platforms may claim they are absolved of responsibility for safety, because they cannot act on what they cannot see.
- Notably, E2EE is just one type of encryption and others have different capabilities and applications, but none are foolproof. How online services and platforms use encryption is not transparent, so it is currently unclear what proactive and preventative steps can and should be taken to safeguard and protect users.

Recent coverage

E2EE has become an increasingly significant online safety concern as large industry players move toward its use, hindering the work of agencies like eSafety and police in detecting and removing the vast amounts of child sexual abuse material and evidence of grooming online.

As noted by eSafety Commissioner Julie Inman Grant in the Weekend Australian Magazine on 7 February 2020, this is a key issue yet to be resolved. As it currently stands, popular services such as WhatsApp and iMessage are fully encrypted and technologies that might detect any child sexual abuse images and videos that are sent over their platforms cannot be used. With Facebook seeking a move to full encryption, the importance of embedding safety into E2EE has never been more important. As stated by the Commissioner, 'We are in an arms race against the worst of the worst' and if platforms don't put safety ahead of money, the cost will be felt most deeply by the abused children left behind.

The eSafety Commissioner's blogpost End-to-end Encryption: a challenging quest for balance (25 February 2020) also explains why the risks can't be ignored, while in August 2019 the Commissioner and Detective Inspector Jon Rouse of the Australian Centre to Combat Child Exploitation (ACCCE) called for a more concerted collective effort to ensure E2EE does not impede the fight against online child exploitation.

E2EE is not inevitable. Facebook's use of E2EE is a few years away, Apple does not encrypt iCloud backups, and Google's E2EE offering to customers is still only opt-in. The issues are very much alive, and we have an opportunity to pave a different path. A letter signed by over 100 child protection organisations and academics across the world highlighted the breadth of community concerns.

eSafety approach

- E2EE requires detailed consideration to minimise the potential for harm across communication channels, and to ensure there is a balance between security, privacy and safety.
- We acknowledge that solutions which threaten to undermine the overall security of the internet are unlikely to work, long term.
- We know there are a number of solutions that would ensure illegal activity online can be addressed, without weakening encryption and still allowing lawful access to information needed in serious criminal investigations. Solutions include:
    - using certain types of encryption that allow proactive tools to function
    - implementing proactive detection tools at transmission, rather than on receipt
    - moving AI and proactive technical tools to the device level.
- We call on industry to commit to, and focus on, detecting illegal content through greater investment in suitable and robust approaches to encryption.
- We call for these protections to be built in from the design stage, not retrofitted once harm has been done. This is known as Safety by Design.
- We call for greater industry transparency before further encryption is introduced, including information about how services will manage risks and fight against illegal content online.
- We recognise that solutions will need to be multi-faceted and require collaboration between industry, government and the general public to be effective. eSafety will apply the necessary pressure and advocate strongly to support safety solutions being built into encrypted services.

Advice for users

Users are advised to take extra care when communicating on encrypted sites, particularly when they do not know the person they are communicating with. It is important to remember that steps can be taken to report, block and mute individuals or accounts on E2EE sites. Also, support is available at eSafety for those who have experienced serious cyberbullying or cyber abuse, have had their intimate images shared or posted without their consent online, or have identified child sexual abuse material or abhorrent violent material online.

All Australians who encounter child sexual abuse images, videos, livestreaming or other content that incites the production or sharing of this type of material on encrypted services should immediately report it to the police.

Australians who encounter other abuse on encrypted services, including serious cyberbullying and image-based abuse, should:

- collect as much evidence as possible — for example, by taking screenshots if it is safe to do so
- report the abuse and the individual or account to the encrypted service
- report the abuse to eSafety
- block or mute the person from being able to contact or interact with them.

Evidence like a screenshot is very important because it helps eSafety to negotiate with the encrypted service to take action against the individual or account responsible for it.

However, please note that possessing, creating or sharing intimate images or videos of people who are under 18 may be unlawful, even if they are intended as evidence of cyberbullying, adult cyber abuse or image-based abuse. For more information about relevant laws in Australia, visit Youth Law Australia.

Published: 25 February 2020
Updated: 11 May 2020