

## Avoiding Wilful Blindness: Safeguards on End-to-End Encryption to prevent online child sexual abuse

April 2024

**Warning:** The following action includes information about sexual violence against children.

The World Council of Churches in their 'Child Safeguarding Policy' offers a theological reflection on the duty of churches to protect children from harm:

*It is the duty and commitment of the church to safeguard and respect all children, not only those inside our church community, without any discrimination or distinction. Our personal authority and responsibility in relation to children are expressed in diakonia, which means self-sacrificial care of their spiritual and physical well-being, following the example of Christ (Philippians 2:5-8; Matthew 25).*

There is a need for the Australian Government to be part of global efforts to ensure that end-to-end encryption is not implemented on social media in a way that increases child abuse and exploitation online.

*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 paedophiles. 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.*

From a survivor quoted by the US National Centre for Missing and Exploited Children, 'End-to-End Encryption: Ignoring Abuse Won't Stop It', <https://www.missingkids.org/e2ee>

Encryption is neither completely good nor bad. The widespread adoption of encrypted web protocols like https has contributed positively. Standard encryption has improved how we can securely browse the web, access banking and government services, and communicate over e-mail and messaging apps. Until recently, privacy and security improvements have mainly been compatible and complementary with the systems protecting the safety of the most vulnerable users.

Deploying end-to-end encryption in communication and social media platforms has a high likelihood of working in direct opposition to protecting the safety of the most vulnerable users. It bypasses the tools technology companies are using to detect child sexual abuse content. End-to-end encryption extends standard encryption so that only the sender and receiver can view the content of messages. Thus, the platforms themselves are prevented from accessing any data being hosted on or passed through their systems. It is important to acknowledge that all popular messaging platforms already use standard encryption, which protects our data from being intercepted by third parties. The only real difference between end-to-end encryption and standard encryption is that the technology platform will no longer have any access to the content. Thus, it will not be able to use tools that can automatically detect images and videos of child sexual abuse that are being hosted or shared on their platforms.

In the first half of 2021, due to an unintended consequence of new EU privacy laws, Meta stopped voluntarily scanning its platforms in the EU. During that time, the US National Centre for Missing and Exploited Children recorded a 58% reduction in reports of online child sexual abuse content. The reduction in detection demonstrates the disastrous consequence to curbing child sexual abuse online if automatic detection tools are blocked by end-to-end encryption.

In 2018, Facebook reported 16.8 million suspected posts and messages related to child sexual abuse on their platforms. In the UK alone, these reports resulted in 3,000 children

being safeguarded from further child sexual abuse and the arrest of 2,500 suspected perpetrators.

The governments of Australia, the UK, and the US stated in 2019 that their technical experts had advised that it was possible to protect users of the platforms and the public while protecting privacy. The response from Meta (the owner of Facebook and Whatsapp) was to reject that view and argue, in effect, that privacy needed to override protecting children from sexual abuse on their platforms. In Meta's view, actions to address online child sexual abuse on their platforms would need to work separately from the implementation of end-to-end encryption.

There was good news on 21 February 2024, with the Australian and UK Governments signing a Memorandum of Understanding that included a commitment "to ensure end-to-end encryption and technologies that aim to enhance privacy and security do not undermine the right to safety, especially for children, and tightly controlled lawful access to data."

There is a need to encourage the Australian Government to stay firm in protecting children from online facilitated sexual abuse by ensuring the use of encryption by social media corporations does not compromise the well-being and safety of children.

### What You Can Do

Write polite and respectful letters to:

**The Hon. Mark Dreyfus KC MP**

Attorney General  
PO Box 6022  
House of Representatives  
Parliament House  
Canberra ACT 2600

Salutation: Dear Minister

**The Hon. Anthony Albanese MP**

Prime Minister  
PO Box 6022  
House of Representatives  
Parliament House  
Canberra ACT 2600

Salutation: Dear Prime Minister

**The Hon. Michelle Rowland MP**

Minister for Communications  
PO Box 6022  
House of Representatives  
Parliament House  
Canberra ACT 2600

Salutation: Dear Minister

**The Hon. Clare O'Neil MP**

Minister for Cyber Security  
PO Box 6022  
House of Representatives  
Parliament House  
Canberra ACT 2600

Salutation: Dear Minister

Points to make in your letters:

- Express concern that social media corporations are moving to implement end-to-end encryption on their platforms in a way that will facilitate an increase in online child sexual abuse on their platforms.
- Ask the Australian Government to continue to work with other governments to ensure that social media corporations:
  - Embed the safety of the public in system designs, thereby enabling them to continue to act against illegal content effectively with no reduction to safety and facilitating the prosecution of offenders and safeguarding of victims;
  - Enable law enforcement to obtain lawful access to content in a readable and usable format;
  - Engage in consultation with governments to facilitate this in a way that is substantive and genuinely influences their design decisions; and,
  - Not implement the proposed changes until they can ensure that the systems they would apply to maintain the safety of their users are thoroughly tested and operational.