Parliamentary Joint Committee on Law Enforcement Inquiry into law Enforcement Capabilities Relating to Child Expoliation Hearing – 15 November 2022

Australian Institute of Criminology response to Questions on Notice:

Question on Notice 1:

Senator SHOEBRIDGE: There are proposed draft codes for the industry that were put out for public submission on 1 September of this year. I know it's not your job to implement them; I know that's primarily being implemented through the eSafety Commissioner. But those codes don't deal with this issue of end-to-end encryption and surveillance within a platform to address the concerns of end-to-end encryption. At least that's my reading of them. Have you had a look at the codes?

Dr Brown: I have. I'm not a lawyer, so my understanding is limited, but my reading of those is that there's a particular focus on two areas. One is the risk analysis, and identifying and understanding the problems. The other, in a wider sense, is reporting and blocking. I actually hadn't identified the lack of the end-to-end encryption aspect in those, but what I did identify was that it's about dealing with the reporting aspects rather than the design of those platforms. So it's the design from the outset that allows for them to be used for the creation and sharing of CSAM. It's those aspects, which, in my reading, the codes are silent on.

Senator SHOEBRIDGE: In fact, absent good design and end-to-end encryption make the secondary responses of reporting and notification next to impossible.

Dr Brown: They would do.

Senator SHOEBRIDGE: So, if we go down a pathway of a code of conduct that's all about responding, reporting and identifying, without addressing the end-to-end encryption problem, we're creating a 20th-century solution to a 21st-century problem, aren't we?

Dr Brown: If that's the case. I would need another reading to make sure that is the case.

Senator SHOEBRIDGE: I heard your caveat earlier, Dr Brown.

Dr Brown: Theoretically, that is the case. We know we see a dip in reporting, and we've got the empirical evidence to show that there's a dip in reporting when end-to-end encryption is introduced. If that becomes the norm on all platforms, then there's a whole lot of material that's going to be produced and shared that those companies won't be aware of and that law enforcement, therefore, won't be able to do anything about.

Senator SHOEBRIDGE: I might give you the opportunity to respond on notice to that issue about end-to-end encryption and the codes, rather than catch you on the hop here.

Dr Brown: Sure.

Response

In July 2022, the AIC published a Trends & Issues research paper titled *Child sexual abuse material and end-to-end encryption on social media platforms: An overview*. This paper reviewed open-source materials including electronic service provider (ESP) transparency reports to provide an overview of the contemporary problem of child sexual abuse material (CSAM) offending on ESP platforms, examine measures currently used by ESPs to detect and prevent CSAM offending, and explore the potential impact of end-to-end encryption on CSAM distribution and detection. The study found that the platforms with the highest user bases are actively detecting and removing CSAM. However, some are less transparent than others about the methods they use to prevent, detect and remove CSAM, omitting key information that is crucial for future best practice in reducing CSAM offending. Further, the adoption of end-to-end encryption by ESPs that detect and remove large amounts of CSAM from their platforms will likely provide a haven for CSAM offenders. Implications for ESPs and international law reform are also discussed (Teunissen & Napier 2022).

The AIC notes the work of the e-safety commissioner in reference to end-to-end encryption and industry codes.

In relation to industry codes, in September 2022, the eSafety Commission released the *Consolidated Industry Codes of Practice for the Online Industry Phase 1* (Industry Codes), which contain specific clauses relating to electronic service providers and their responsibilities in protecting users and the public (Online Safety 2022a).

The Industry Codes make specific reference to encryption only in relation to 'relevant electronic services' (platforms used for messaging), no other services listed (social media services, designated internet services, internet search engine services, App distribution services, Hosting services, internet carriage services, Manufacturing, supplying, maintaining or installing equipment).

The Industry Codes refer to 'encrypted relevant electronic services' as being relevant electronic services that are entirely end-to-end encrypted, or those that allow communications between end-users (the users of these platforms and products) that are end-to-end encrypted (e.g. WhatsApp). This excludes 'closed communication relevant electronic services' (see Table 2 for explanation of key terms).

The Industry Codes refer to online content categorised as Class 1A and Class 1B Material (see Table 2), which are subcategories of Class 1 Material (eSafety 2021).

Table 2: Description of terms	
Class 1A Material	Child sexual exploitation material, pro-terror material, and extreme crime and violence material
Class 1B Material	Crime and violence material and drug-related material
End-user	Users of electronic services, platforms, and/or products
Closed communication relevant electronic service	A relevant electronic service that enables an Australian end-user to access and communicate with a list of contacts created by the end-user but does not: a) enable them to view, navigate or search for others on the service without already having their contact details; or b) recommend other contacts to end-users based on interests or shared connections.

Encrypted relevant electronic service	A relevant electronic service which is entirely end-to-end encrypted, or where the communications between end-users are end-to-end encrypted (excludes closed communication relevant electronic services).

Source: Online Safety 2022b.

Per section Section 5 and clause 5(d) of the Industry Codes (Online Safety 2022a: pp. 4-5), these services must undertake a risk assessment to assess the risk posed to Australian end-users that class 1A and 1B material will be accessed, distributed or stored on the service, and determine whether the risk profile of this occurring on the service is low, medium, or high. If a provider changes their service(s) so that they would be considered an encrypted relevant electronic service, they must conduct a risk assessment in accordance with this clause. These risk assessments must be documented and clearly explain the methodology used to determine the risk profile, and the process by which the assessment was carried out. Risk assessments must be reviewed following implementation of any significant features that may result in increased risk for the service. Risk assessments must include (at a minimum) functionality, purpose and scale of any relevant electronic service.

Providers of encrypted relevant electronic services must comply with the minimum compliance measures as listed for encrypted relevant electronic services in clause 7(a) and specified in the table in clause 8 (see Online Safety 2022a, pp. 10-21). This table is summarised at a high level in Table 3, outlining the minimum compliance measures that encrypted relevant electronic services must provide as per the Industry Codes. Please see Online Safety (2022a) for full detail on each of these measures.

Table 3: Minimum compliance measure that encrypted relevant electronic services must provide	
#	Measure
2	Notifying appropriate entities about CSEM and pro-terror material on their services
3	Systems and processes for responding to violation of policies prohibiting CSEM and pro-terror material
4	Systems and processes for responding to violation of policies (class 1A materials other than CSEM and pro-terror materials)
6 & 13	Trust and safety function
7	Safety features and settings
11	Systems and processes for enforcement of policies
15	Forum with other industry participants
17	Updates and consultation with eSafety about relevant changes to technology
18	Information for Australian end-users about the role and functions of eSafety, including how to make a complaint to eSafety
19	Reporting and complaints mechanisms for class 1A and class 1B material
20	Complaints about handling of reports and/or compliance with Code
22	Publication of policies relating to the OSA
28	Respond to written requests from eSafety regarding the steps that the provider has taken to comply with their applicable minimum compliance measures and an explanation as to why these measures are appropriate

from Online Safety 2022a (pp. 10-21).

Question on Notice 2:

Senator SHOEBRIDGE: Could I also ask you to provide on notice what you know about and any numbers you have on the reduction in reporting that coincided with the different platforms adopting end-to-end encryption.

Dr Brown: We can provide that.

Senator SHOEBRIDGE: Thanks.

Response

The AIC refers to data published by the National Centre for Missing and Exploited Children (NCMEC), based in the United States and the Internet Watch Foundation (IWF) in the United Kingdom

Table 1 depicts the number of reports of child sexual exploitation received by the NCMEC and the IWF from 2014 to 2021. The majority of these reports pertain to child sexual abuse material (CSAM). Additionally, these data clearly demonstrate an upward trend in the number of reports received by both entities across an eight-year period. Table 1 also outlines the companies/platforms that implemented end-to-end encryption (E2EE) in each of these same calendar years.

Table 1: Number of NCMEC and IWF child sexual exploitation reports, and implementation of encryption on large online platforms between 2014–2021

Year	# NCMEC Reports of CSAM	# IWF Reports of CSAM	Companies/platforms that first introduced E2EE in this year
2014	1,100,000	74,119	
2015	4,400,000	112,975	
2016	8,200,000	105,420	WhatsApp Facebook Messenger (optional & limited[b])
2017	10,200,000	132,636	
2018	18,462,424	229,328	Skype
2019	16,987,361	260,426	Snap Inc
2020	21,751,085	299,619	Google (Messages)
2021 [a]	29,397,681	361,062	Microsoft Teams (optional & limited[c])

Notes: Data and references obtained from Teunissen & Napier 2022 unless otherwise specified.

a: Data from IWF 2022 & NCMEC 2022

b: Meta implemented the option for users to enable end-to-end encryption in one-on-one Messenger conversations in 2016. Global rollout of end-to-end encryption enabled by default on all Messenger conversations has been delayed to 2023 (Davis 2021)

c: Users/network administrators must enable end-to-end encryption and this is limited to one-on-one conversations

Source: see Teunissen & Napier 2022

Basic Online Safety Expectations and relevance of encryption

As per Subsection 8 of the *Online Safety (Basic Online Safety Expectations) Determination 2022* (Cth), it is expected that a provider (a social media service, other relevant electronic service of any kind, or designated internet service of any kind) will take reasonable steps regarding encrypted services:

> (1) If the service uses encryption, the provider of the service will take reasonable steps to develop and implement processes to detect and address material or activity on the service that is unlawful or harmful.
>
> (2) Subsection 8(1) does not require the provider of the service to undertake steps that could do the following:
>
> (a) implement or build a systematic weakness, or a systematic vulnerability, into a form of encrypted service;
>
> (b) build a new decryption capability in relation to encrypted services; or
>
> (c) render methods of encryption less effective

References

All references working as of 17 November 2021.

Davis A 2021. We'll protect privacy and prevent harm, writes Facebook safety boss. The Telegraph, 20 November. https://www.telegraph.co.uk/business/2021/11/20/people-shouldnt-have-choose-privacy-safetysays-facebook-safety/

eSafety 2022. eSafety issues first Basic Online Safety Expectations notices. https://www.esafety.gov.au/industry/basic-online-safety-expectations

eSafety 2021. Online Content Scheme Regulatory Guidance. eSC RG 4. https://www.esafety.gov.au/sites/default/files/2021-12/eSafety-Online-Content-Scheme.pdf

Internet Watch Foundation 2022. IWF Annual report 2021. https://www.iwf.org.uk/about-us/who-we-are/annual-report-2021/

Kricheli R 2021. Messenger Updates End-to-End Encrypted Chats with New Features. https://messengernews.fb.com/2021/08/13/messenger-updates-end-to-end-encrypted-chats-with-new-features/

Malik M 2021. Use end-to-end encryption for one-to-one Microsoft Teams calls. https://techcommunity.microsoft.com/t5/microsoft-teams-blog/use-end-to-end-encryption-for-one-to-one-microsoft-teams-calls/ba-p/2867066#:~:text=UPDATE%3A%20As%20of%20December%2015,support%20for%20Microsoft%20Teams%20Calls

National Center for Missing and Exploited Children 2022. CyberTipline 2021 Report. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

Online Safety 2022b. Head terms for all code schedules. https://onlinesafety.org.au/codes/

Online Safety 2022a. Relevant electronic services. https://onlinesafety.org.au/codes/

Teunissen C & Napier S 2022. Child sexual abuse material and end-to-end encryption on social media platforms: An overview. *Trends & issues in crime and criminal justice* no. 653. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78634