IJM

International Justice Mission Australia
Response to Questions on Notice

Joint Select Committee on
Social Media and Australian Society

Questions from Mr Andrew Wallace MP, Federal Member for Fisher

14/11/2024

International Justice Mission (IJM) Australia appreciates the opportunity to provide written responses to the following questions taken on notice at the public hearing of the Joint Select Committee on Social Media and Australian Society on 30 September 2024.

You talk a lot about online exploitation, including scams, which involve romantic relationships or even romance and dating apps. These kinds of apps continue to grow in use in Australia.

- **How should the Government respond to the growing use of these apps and platforms for the sexual and financial exploitation of Australians, including children?**

IJM estimates that romance cryptocurrency investment scams are among the largest type of scam powered by modern slavery in Southeast Asian scam compounds. At least 300,000 people are estimated to be engaged in the scamming industry in the Mekong region alone[1], an industry rife with allegations of labour trafficking and other human rights abuses.

Romance scams usually occur when a remote third party reaches out to an Australian via a dating app or 'missed connection' message. If the Australian target engages in the conversation, the scammer attempts to move the conversation over to a different end-to-end encrypted messaging platform where they can introduce cryptocurrency investment into the conversation without leading to flags on the dating app platform.

According to the National Anti-Scam Centre, Australians lost $210.2 million to romance scams in 2022[2] and $201.1 million in 2023[3]. IJM welcomes this downward trend and acknowledges that romance scamming is still as significant problem in Australian society.

Dating apps and other social media platforms must collaborate closely with government to stem romance scamming, which is resulting not only in financial damage to Australians but significant legal and reputational risks for dating platforms' failure to keep their users safe. Government should encourage dating apps to use internal tools to disrupt and prevent the further growth of online scamming.

For example, the Government should require dating apps to proactively identify and ban users seeking to perpetrate online scams. Government could also require dating platforms to provide pop up scam warning messages if Australian users receive a message from another user prompting them to move their conversation over to another platform or to exchange

[1] [1]https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

[2] https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf

[3] https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf

personal contact details. These changes could be implemented through a future review of the recently commenced voluntary Online Dating Industry Code or incorporated into the Scams Prevention Framework.

In addition, the online sexual exploitation of children can even take the form of livestreamed child sexual abuse, whereby adult offenders in western countries, such as Australia, pay traffickers in low income countries to commit contact sexual abuse of often young children while offenders pay for and direct this abuse in real time.

Europol's 2024 Organized Crime Threat Assessment reports: "Live-distant child abuse (LDCA) is a persistent threat, where offenders watch child sexual abuse on demand with the support of one or more facilitators who perpetrate the abuse on the victim(s) in exchange* for payment. It stands out as the main form of commercial sexual exploitation of children and as a major source of unknown** CSAM using capping, which entails covertly recording the victim (i.e. in a video call/live-streaming session)."[4]

Dating platforms

In cases of livestreamed child sexual abuse, online sessions are solicited and arranged by the perpetrator and the facilitator using everyday social media platforms, including dating apps and adult webcamming sites.[5] The livestreamed abuse sessions are often conducted through popular platforms such as Microsoft Skype, Facebook Messenger and WhatsApp.[6]

According to a 2023 scoping review, "it is common for Filipino traffickers to seek out and connect with demand-side offenders ("customers") on social media platforms to offer and sell them livestreamed child sexual abuse of Filipino children, along with child sexual abuse images and videos (CSAM). Adult dating websites and adult webcam sites are also common places for solicitation and should not be overlooked."[7]

Research published in 2024 by Justice & Care in partnership with IJM also supported these conclusions. The study notes:

- "Most traffickers communicated and exchanged materials with customers on the surface of the worldwide web (as opposed to the dark web). Often, they used platforms, such as social media or personal messaging sites, email, dating websites, or adult websites..."[8]
- "There are references to 'chatting' to foreigners through social media platforms or dating websites such as Filipino Cupid, Cherry Blossoms, and Asian Dating."
- "Relatedly, concerted action is required to target online dating sites and adult webcam services identified in this analysis as being implicated in OSAEC crimes (e.g. used to foster and develop foreign perpetrator-local facilitator connections to commission OSAEC, subsequent live streaming of OSAEC and other OSAEC crimes against Filipino children). These actions should, inter alia, encompass regulation and

[4] https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf, pg. 26

[5] https://justiceandcare.org/policies-and-reports/facilitation-of-online-sexual-abuse-and-exploitation-of-children-osaec-in-the-philippines/

[6] "Legal and institutional responses to the online sexual exploitation of children," University of Nottingham Rights Lab, September 2023, https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/legal-and-institutional-responses-to-the-online-sexual-exploitation-of-children-the-united-kingdom-country-case-study.pdf, page 10.

[7] https://www.sciencedirect.com/science/article/pii/S0190740923000567

[8] Facilitation of Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines - Justice and Care

> investigation of these platforms and services and targeted, platform-level activity to detect and report potential on-platform OSAEC."

These conclusions are supported by IJM's extensive experience in the Philippines, supporting law enforcement in 438 operations, leading to the arrest of 423 suspects and the rescue of over 1,378 victims and at-risk individuals (as of 25 September 2024).

To counter the use of dating apps by Australian offenders to solicit livestreamed child sexual abuse, the Government should require dating app companies to proactively detect suspicious conversations using known keyword indicators for review and reporting to law enforcement. Dating app companies should ban users who have attempted to solicit child sex abuse material on their platforms and prevent recidivism. These changes could be implemented through a future review of the recently commenced voluntary Online Dating Industry Code or RES Codes under the Online Safety Act.

Additionally, Government should incentivise social media companies to join initiatives such as Project Lantern, which enables signal sharing among tech platforms to understand when child sexual abuse may be taking place.

- **What information would organisations and researchers at IJM and others in the sector need from social media companies, dating apps, gaming platforms, streaming platforms, messaging apps and similar digital platforms in order to better understand the prevalence of, and support the prevention and prosecution of child sexual abuse and exploitation?**

In IJM's submission to the Online Safety Act review, we recommended the following measures.

- The Government should require digital services and platforms who are not currently making reports of suspected and actual child sexual exploitation material to the National Center for Mission and Exploited Children to report these to the Australian Federal Police and/or the National Center for Missing & Exploited Children, even if not legally mandated to do so by US law. This supports the global ecosystem of reporting and international collaboration with law enforcement agencies globally.

- The Government should provide the eSafety Commissioner with powers to mandate the type of information to be included in the reports and the timeframe for sending those reports to ensure that they are useful for law enforcement investigation. IJM is prepared to provide recommended reportable data points that may expedite investigations into suspected online sexual abuse and exploitation of children.

- The Government should establish detailed record keeping and content preservation requirements, and more appropriate penalties for failure to report content in line with requirements under online industry codes and standards in line with comparative international legislation.

You cite the Australian Institute for Criminology's research which named Skype, Messenger and WhatsApp as platforms which offenders in Australia and the UK are using to livestream child sexual abuse and exploitation.

Skype, Messenger and WhatsApp are known to be popular apps by which offenders livestream child sexual abuse material. Attributions of the source material for these findings are as follows:

- A 2021 study by the Australian Institute for Criminology found that popular video call platforms such as Facebook Messenger and Skype have been used by Australian men to view the livestreamed sexual abuse of children in vulnerable countries.[9]
- The University of Nottingham's Rights Lab published a study in 2023 that documented 30 cases beginning in 2010 involving UK offenders using platforms Microsoft Skype, Facebook Messenger, and WhatsApp to livestream child sexual abuse.[10]
- A 2023 scoping review identified relevant electronic services such as Skype and Facebook Messenger as well-established platforms used to initiate and facilitate live streamed child sexual abuse.[11]

- **What should Microsoft and Meta do immediately to stop CSAM, CSEM and livestreamed abuse on these platforms?**

According to the eSafety Commissioner's first transparency report published in December 2022 which covered Meta and Microsoft, "eSafety's understanding from their responses to the notice questions is that the providers are neither taking action to detect CSEA [child sexual exploitation and abuse material] in livestreams … or taking action to detect CSEA in video calls or conferences."[12]

In their responses to eSafety's transparency notice, Meta disclosed it was using proactive detection tools for new CSEA on Messenger but not livestreamed content, whilst Microsoft did not have any tools in place to detect new or livestreamed CSEA on Skype.[13]

In IJM's submission to the Online Safety Act Review, we recommended that digital platforms be required to have accurate systems that detect when child sexual exploitation and abuse content is shared using their platforms. Tech companies should be able to detect and take action immediately and block accounts that use the platforms to abuse children.

We also recommend that digital services be held accountable for livestreaming child sexual abuse – that such criminal activity be proactively detected and disrupted on their platforms. If possible, applications that do not detect and stop the abuse should be shut down from public access.

Instagram's client-side scanning initiative, which works even in encrypted platforms, should be implemented across the board to detect and prevent the sharing, production, and creation of child sexual abuse material. Mandatory deployment of this client side scanning technology which companies like Meta, WhatsApp and Apple are already using should be targeted to prevent child sexual abuse.

Meta-owned Instagram likewise reports that:

> "Nudity protection uses on-device machine learning to analyze whether an image sent in a DM on Instagram contains nudity. Because the images are analyzed on the

[9] Napier, Teunissen & Boxall (2021), Live streaming of child sexual abuse: An analysis of offender chat logs (aic.gov.au)

[10] "Legal and institutional responses to the online sexual exploitation of children," University of Nottingham Rights Lab, September 2023, https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/legal-and-institutional-responses-to-the-online-sexual-exploitation-of-children-the-united-kingdom-country-case-study.pdf, page 10.

[11] https://pubmed.ncbi.nlm.nih.gov/36727734/

[12] https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf

[13] https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf

> device itself, nudity protection will work in end-to-end encrypted chats, where Meta won't have access to these images."[14]

Similarly, "WhatsApp automatically performs checks to determine if a link is suspicious. To protect your privacy, these checks take place entirely on your device. Remember, because of end-to-end encryption, WhatsApp can't see the content of your messages."

Clearly, it is possible to address child exploitation online while preserving user privacy—the principles and tools just need to be applied across the board.

- **Which other platforms are being used based on your research and experience?**

The 2018 Europol Internet Organized Crime Threat Assessment says " Peer-to-peer sharing platforms such as Gigatribe, BitTorrent and eDonkey remain the most common communication channels for the dissemination of CSEM, although there is some evidence tosuggest this is decreasing. More general, everyday communication applications with end-to-end encryption, such as WhatsApp and Telegram, are also frequently used. Some law enforcement agencies also see traditional email services being used to send and receive CSEM. Finally, there appears to be a rise in the distribution of CSEM on everyday social media platforms."[15]

Skype and Messenger are key platforms where livestreamed CSAM is occurring, but it is so important to note that OSEC is happening on platforms that most legislators wouldn't dream of - such as on school websites. Therefore, it is important to swim as far upstream as possible and think about making devices safe by design, as unsafe devices are allowing these crimes to flourish. A mobile phone, laptop, or tablet should never be able to render, create, and distribute CSAM.

In February 2024, Finnish NGO Protect Children published findings of a survey of dark web offenders to understand offending patterns and identified that social media platforms are commonly used to search for and view sexually abusive images and videos of children.[16]

Findings include:

- One in three respondents to their survey of individuals searching for CSAM on dark web search engines reported that, alongside using the dark web to find CSAM, they have also actively used popular social media platforms to view and share the imagery.
- Of the social media platforms presented in the survey, the top platforms used by respondents to search for, view, or share CSAM were Instagram (29%), which was used by nearly a third of respondents, X (Twitter) (26%), and Discord (23%). Discord, TikTok, and Facebook, and are each used by at least one in five respondents to view CSAM.
- Other social media platforms mentioned by survey respondents in response to the option "Other, what?" included Telegram and WhatsApp, which, although primarily messaging apps, also offer social networking features. The majority of the social media platforms mentioned also offer private and group messaging functions. There is an unmistakable overlap between the social media platforms most used for viewing

[14] https://about.fb.com/news/2024/04/new-tools-to-help-protect-against-sextortion-and-intimate-image-abuse/
[15] https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf
[16] https://bd9606b6-40f8-4128-b03a-9282bdcfff0f.usrfiles.com/ugd/bd9606_0d8ae7365a8f4bfc977d8e7aeb2a1e1a.pdf

and sharing CSAM and the platforms most popular among children and young people.

- In 2023, a group of male adolescents in Spain allegedly 'nudified' images of over 20 girls and adolescents and shared them via WhatsApp and Telegram. Similar cases have since been reported in Australia. In an attempt to tackle this, TikTok and Meta have blocked popular search terms associated with nudification tools.
- In addition to social media platforms, the researchers found that many respondents used messaging apps to view and share CSAM. Telegram was by far the most popular messaging app mentioned (46%), followed by WhatsApp (37%).
- Nearly half of respondents who had used a messaging app to view and disseminate CSAM reported that they used Telegram. According to its Terms of Service, the platform explicitly forbids the posting of "illegal pornographic content on publicly viewable Telegram channels, bots, etc.", however it does not explicitly forbid this in private channels.[17]
- The UK Online CSEA Covert Intelligence Team reports Telegram to be one of the most trusted platforms for the sharing of illegal imagery, as well as for offender to offender communication.[18] It is commonly used by first-generation producers and for live-streaming of abuse. The messenger does not disclose any data to third parties, including governments, and has many privacy features that appeal to offenders such as end-to-end encryption, secret chats, self-destruct messages, editing and deleting any message from all devices after sending or receiving it, and private groups and channels.[19]
- 37% of respondents shared that they established the first contact with a child via a messenger, mostly via end-to-end encrypted messengers Telegram (45%) and WhatsApp (41%).

David Braga
Chief Executive Officer

Grace Wong
Chief Advocacy Officer

[17] Terms of service. (n.d.). Telegram. https://telegram.org/tos.

[18] Material provided by the UK Online CSEA Covert Intelligence Team

[19] Telegram FAQ. (n.d.). Telegram. https://telegram.org/faq?setln=en#q-there39s-illegal-content-on-telegram-how-do-i-take-it-down.