Australian National University

August 2021
National Security College

Public Submission - Parliamentary Joint Committee on Law Enforcement - Law enforcement capabilities in relation to child exploitation

Submission made on behalf of
Dr. William A. Stoltz of the
National Security College, Australian National University

Introduction

I wish to thank the Committee for the opportunity to provide this submission to inform the Committee's inquiry into the ability of Australia's law enforcement agencies to prevent, detect, and respond to instances of child exploitation, particularly online. For the avoidance of doubt, the views conveyed in this submission are those of the author alone and should not be taken to represent an institutional position on behalf of the National Security College, nor the Australian National University.

This submission argues that recent legislative proposals by the Australian Government have, in effect, positioned the problem of online child exploitation in parallel with national security threats, owing to the harmful impact of online child exploitation on the wellbeing and values of Australian society.

Additionally, this submission suggests that the communication services provided by Facebook Inc. (Messenger, Instagram, WhatsApp, and the eponymous Facebook platform) are of such a significant scale and are so uniquely pertinent to the problem of online child exploitation, that Facebook Inc. should be the subject of special scrutiny and regulation by the Commonwealth. In particular, I argue that Facebook Inc.'s adoption of end-to-end encryption (E2EE) across its services shows that the Commonwealth needs to explore options for regulating the accessibility of encrypted communications services according to different contexts; primarily, whether it is appropriate for otherwise publicly moderated social media communications involving minors to seamlessly transition into secret encrypted communications within the one ecosystem.

Accordingly, this submission offers the Committee the following recommendations to compliment the work of law enforcement agencies and hopefully make the operating environment less permissive to offenders targeting children.

Summary of Recommendations

- Facebook Inc. should be declared a carriage service provider (CSP) as per section 87 of the *Telecommunications Act 1997* (Telco Act); and

- Parliament should amend the Telco Act to create a power similar to section 315A of the Act that would empower the Minister for Home Affairs to direct a CSP to cease its operations where the provision of its services are found to be prejudicial to the welfare of children; and

- Facebook Inc. should be required to report annually to the Commonwealth's eSafety Commissioner to show that it is satisfactorily mitigating risks to children. Where the Commissioner finds Facebook Inc. is failing to do so, the Commissioner should have the ability to recommend to the Minister for Home Affairs that it be directed to cease its functions as a CSP.

- Separate from the above, the Government should commission the Department of Home Affairs and the Department of Infrastructure, Transport, Regional Development and Communications to explore the feasibility, and options for, regulating the availability of encryption according to the context of its use, with the view to restricting the ability of CSPs to facilitate unsolicited communications with minors that are end-to-end encrypted.

Should it benefit the Committee's further consideration of this topic and these recommendations, I would be happy to make myself available to attend any public hearings the Committee may wish to convene.

Thank you for taking the time to consider my submission.

Sincerely,

Dr. William A. Stoltz
Senior Adviser for Public Policy
National Security College, ANU

Child Exploitation Harmful to the National Interest

Through legislation currently before the Parliament, the Australian Government is signalling a commitment to recognise that child exploitation offences, particularly those conducted online, are so harmful to the wellbeing and values of Australian society that they are affecting the national interest. The *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (SLAID Bill) provides new, extraordinary powers to the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police (AFP) to combat serious offences online, with a specific focus on child exploitation, terrorism, as well as drugs and firearms trafficking.[1] These new powers will allow the ACIC and the AFP to more easily collect intelligence and evidence in relation to malicious criminal networks operating online and, in certain circumstances, perform offensive-style digital disruption to prevent criminal behaviour.

That the Government wants the ACIC and the AFP the use the same extraordinary powers to deal with child exploitation which they will use against national security threats like terrorism and organised crime, demonstrates a new commitment to regard child exploitation as similarly harmful to the national interest as those national security threats. In particular, the SLAID Bill's creation of a data disruption warrant marks a turning point in how Australian agencies will be able to respond to child exploitation; moving from a law enforcement-style response to one where agencies will be able to generate national security-style effects against child exploitation networks. This is because the data disruption warrant does not facilitate evidentiary or intelligence collection. Rather, it allows for the performance of offensive-style data disruption activities akin to the offensive cyber actions performed by the Australian Signals Directorate, whereby the ACIC and/or AFP will be able to delete, degrade, or modify data to prevent it being accessible or being shared.

The Government's commitment via the SLAID Bill to treat online child exploitation as warranting special, significant powers, invites us to consider what additional creative legislative measures might be introduced to assist law enforcement in countering this issue.

Facebook Inc. and Child Exploitation

Based on data accumulated by National Centre for Missing and Exploited Children (NCMEC) in the United States, Facebook Inc. accounts for the overwhelming majority of reported instances of new child abuse imagery detected online.[2] For Australia, this is replicated in AFP reporting.[3] This is likely due in part to high degrees of self-reporting by Facebook Inc. as compared with other technology

[1] Commonwealth Parliament; Parliament House, Canberra 'Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020', Australia, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6623.
[2] Tom Gillespie, 'Facebook Responsible for 94% of 69 Million Child Sex Abuse Images Reported by US Tech Firms', Sky News, 12 October 2020, https://news.sky.com/story/facebook-responsible-for-94-of-69-million-child-sex-abuse-images-reported-by-us-tech-firms-12101357.
[3] Anthony Galloway, 'Facebook Accounts for up to 60% of Child Abuse Reports to AFP, Data Shows', The Sydney Morning Herald, 23 July 2020, https://www.smh.com.au/politics/federal/facebook-accounts-for-up-to-60-percent-of-child-abuse-reports-to-afp-data-shows-20200723-p55ep7.html.

companies. However, Facebook Inc.'s over-representation in these and similar statistics is also certainly because of the unmatched scale and the almost perfect suitability of their platforms for the practice of grooming minors. In particular, I refer to Facebook Inc.'s decision to create a seamless pathway between public social media communications (the Facebook platform and Instagram) to encrypted, secret messaging (Messenger and Instagram messaging).

Currently, the Facebook platform is an ideal environment for those seeking to groom children because they can identify and target minors' profiles on the open Facebook platform but communicate with them via Messenger where, with the increasing roll-out of end-to-end encryption (E2EE), their interactions will be secret. Messenger is directly linked to the Facebook platform and to a user's publicly searchable Facebook profile. Everything a user may post on their profile or the wider platform is visible to other, if not all, users and is not encrypted; meaning communications on the Facebook platform can be moderated. Facebook Inc.'s plans to expand the availability of E2EE for Messenger, including on group discussions as well as video and voice calls,[4] is cementing a glide path for users' communications to seamlessly transition from a largely public environment where they can be moderated, to a closed environment where communications will increasingly be subject to E2EE, rendering them secret. While many adult users may be expected to recognise when their interactions have transitioned to an encrypted environment, children using Facebook Inc. platforms cannot be expected to recognise when interactions have crossed this threshold, and despite Facebook Inc.'s current efforts a large number of minors continue to have access to their platforms; a fact that is being actively exploited by offenders seeking to find, target, and groom children online.

Sadly, Facebook Inc. is exacerbating this problem by also rolling out E2EE to the direct messaging component of Instagram, another platform where minors' profiles can be publicly discoverable. Compounding this further still are Facebook Inc.'s initiatives to implement 'cross-app messaging' and 'ephemeral messaging', respectively.[5]

Cross-app Messaging

Cross-app messaging is allowing encrypted communications to seamless transition from Messenger to Instagram messaging, and potentially to Facebook Inc.'s other platform, WhatsApp.[6] This would mean that one user can send an E2EE message from their Messenger account to another users Instagram message account, and vice versa. Not only does this make interactions even harder to track for Facebook Inc. and law enforcement, but it expands the options for offenders to shift public interacts with children on to secret E2EE channels.

---

[4] Ruth Kricheli, Director of Product Management, and Messenger, 'Messenger Updates End-to-End Encrypted Chats with New Features', *Messenger News* (blog), accessed 16 August 2021, https://messengernews.fb.com/2021/08/13/messenger-updates-end-to-end-encrypted-chats-with-new-features/.

[5] 'Say 👋 to Messenger: Introducing New Messaging Features for Instagram', *About Facebook* (blog), 30 September 2020, https://about.fb.com/news/2020/09/new-messaging-features-for-instagram/.

[6] 'Facebook Introduces Cross-App Communication between Messenger and Instagram, plus Other Features', *TechCrunch* (blog), accessed 16 August 2021, https://social.techcrunch.com/2020/09/30/facebook-introduces-cross-app-communication-between-messenger-and-instagram-plus-other-features/.

Ephemeral Messaging

With regards to ephemeral messaging, this function will allow Messenger, Instagram, and WhatsApp users to set rules for automatically deleting their message history after a certain period of time. This will have incredibly detrimental effects for law enforcement investigations by allowing offenders to easily destroy evidence of their efforts to groom minors, meaning that even in instances where a child or their parent is able to recognise malicious interactions online, it may not be possible for them to substantiate this for police, as the records will be destroyed. Accordingly, this may well have the perverse effect of emboldening offenders to more actively target more minors online because of the reduced likelihood of evidence of their offending being detected.

E2EE, cross-app messaging, and ephemeral messaging are not in and of themselves entirely insurmountable technologies for Australian law enforcement agencies. However, Facebook Inc.'s decision to combine these technologies and seamlessly integrate them into otherwise public social media platforms used by children, not only creates an online environment that is wickedly non-permissive for law enforcement but one that is also perniciously favourable for the practice of grooming children. These decisions by Facebook Inc. put paid to claims by Facebook Inc. that it has a zero-tolerance approach to child exploitation occurring on their platforms.[7] These decisions by Facebook Inc. also warrant the company being specially regulated by the Commonwealth to better ensure they address into the future the unique way in which their platforms can be used for child exploitation at a vast scale. Such special regulation of a corporation is not unprecedented, as Telstra's special status in the *Telecommunications Act 1997* shows.

Regulatory Options for the Commonwealth

Existing Commonwealth legislation in the form the *Telecommunications Act 1997* (Telco Act) provides a pathway for the Parliament to regulate Facebook Inc. in a manner that is not only more appropriate for the services it provides, but that could help to improve law enforcement outcomes against the scourge of online child exploitation.

Recognising Facebook Inc. as a Carriage Service Provider (CSP)

This Committee should call on the Minister for Communications to declare Facebook Inc. a carriage service provider as per section 87 of the Telco Act.[8] Doing so would not only more appropriately recognise the reality of Facebook Inc.'s telecommunications services, but it would also open avenues for the Commonwealth to hold Facebook Inc. more accountable for the role its services play in enabling online child exploitation.

[7] 'PNG: Claims Facebook Isn't Doing Enough to Stop Abusive Content', Sound, ABC Radio Australia (Australian Broadcasting Corporation, 28 July 2020), https://www.abc.net.au/radio-australia/programs/pacificbeat/png-fb-child-abuse/12497882.
[8] 'Telecommunications Act 1997' (Attorney-General's Department), http://www.legislation.gov.au/Details/C2021C00237/Html/Volume_1.

The Telco Act defines as a 'carriage service' as "*a service for carrying communications by means of guided and/or unguided electromagnetic energy*".[9] Further, the Act explains that an organisation or person is a 'carriage service provider' if:

> "*…a person supplies, or proposes to supply, a listed carriage service to the public using:*
> *(a) a network unit owned by one or more carriers; or*
> *(b) a network unit in relation to which a nominated carrier declaration is in force*;"[10]

Based on these definitions within the Telco Act, the Commonwealth should regard Facebook Inc. as an 'over the top' CSP, given it uses the internet network infrastructure put in place by other telecommunications companies, rather than its own, to provide a listed carriage service.

Were Facebook Inc. only operating its Facebook social media platform, it would perhaps be conceivable that Facebook Inc. could skirt being defined as a CSP because this platform could be described more as some kind of online public notice board, rather than a conventional telecommunications listed carriage service like that provided by Telstra or Optus. However, Facebook Inc.'s operation of bespoke user-to-user messaging platforms, like Messenger, Instagram messaging, and WhatsApp, inclusive of encrypted text, video, and voice exchange, makes its services indistinguishable from the communications services provided by other CSPs.

Not only would declaring Facebook Inc. a CSP be an appropriate recognition of the services it currently operates, but it would also create a path for the Commonwealth to better regulate this international technology giant.

Replicating Section 315A of the Telco Act to Protect Children

Section 315A of the Telco Act allows the Minister for Home Affairs, based on an adverse security assessment by the Australian Security Intelligence Organisation (ASIO), to order a CSP to cease its services where its operations are found to be prejudicial to security.

In keeping with the Government's recognition via the SLAID Bill that online child exploitation is significantly harmful to Australia's national values and interests, this Committee should recommend to the Government that the Telco Act be amended to create a provision similar to Section 315A for the purposes of protecting the safety of children. In particular, the Minister for Home Affairs, based on advice from the Commonwealth's eSafety Commissioner, should be empowered to direct a CSP to cease its services where its operations are found to be prejudicial to safety of children. This would mean that, were Facebook Inc. to be declared a CSP, it could be ordered to cease its services in Australia if it does not sufficiently mitigate the risk of child exploitation arising from its platforms.

Furthermore, to allay concerns and avoid the Commonwealth needing to take such a measure, this Committee should also recommend that Facebook Inc. be asked to report to the eSafety Commissioner on an annual basis to show how they are working to mitigate the risk of child exploitation occurring on their platforms and demonstrate why they should continue to be able to operate as a CSP in Australia.

[9] Ibid.
[10] Ibid.

Towards Context Dependent Encryption

Encryption has an important role to play in modern communications and as consumers we should be free to use encrypted communication platforms. However, not all communications are created equal. Whether it be the exchange of commercial or banking information, government deliberations, or discussions between journalists and their sources, some communications should rightly be encrypted for secrecy, but some should not. In particular, social media communications do not need to be subject to E2EE and those involving minors as a rule should not be. Instead, the accessibility of E2EE should be context dependent.

The persistent problem of minors being groomed via Facebook Inc.'s platforms is a key example why this should be the case, because at the moment it is permissible and easy for an otherwise unrelated adult to make unsolicited contact with a minor via an online public profile before shifting their engagement into an encrypted, secret context.

To explore options for addressing this, the Committee should recommend that the Government commission the Department of Home Affairs and the Department of Infrastructure, Transport, Regional Development and Communications to explore the feasibility, and options for, regulating the availability of encryption according to context, with the view to finding ways to restrict the ability of CSPs to facilitate unsolicited communications with minors that are end-to-end encrypted. This is not to say that parents could not provide an encrypted channel for communicating with their children, but that an avenue simply need not and should not exist for a child to be approached publicly on social media and, without their guardian's agency, be brought into an encrypted environment.

About the Author

Dr. William A. Stoltz

Dr. Stoltz is the Senior Adviser for Public Policy at the National Security College, ANU. He is responsible for mobilising the College's research and resident expertise to influence and inform current public policy debates.

Dr. Stoltz's own research explores options for Australia to shape and influence international security, as well as Australia's policy responses to a breadth of domestic national security challenges.

He holds a PhD and Advanced Masters of National Security Policy from the Australian National University as well as a Bachelor of Arts from the University of Melbourne.