PARLIAMENT OF AUSTRALIA

Parliamentary Joint Committee on Law Enforcement

Law Enforcement capabilities in relation to child exploitation
Public Hearing – 10 December 2021
Questions on Notice
Communications Alliance

1 QUESTION 1. Committee Hansard, pp. 16-17

CHAIR: Thank you very much. We've heard varying reports from different law enforcement jurisdictions about the time it takes to solicit cooperation out of various tech providers. I was wondering if, given your role, you had any data you could provide the committee with on how often law enforcement requests are made to your members and the response times they have for those?

Ms Gillespie-Jones: Can I ask whether the law enforcement agencies' evidence made any distinctions as to whether it was talking about platforms or internet service providers and current service providers?

CHAIR: They were primarily referring to platforms.

Ms Gillespie-Jones: We don't have any data specifically as to how long it takes. My understanding, though, is that the larger platforms that are our members react quite quickly; that's the feedback we have received.

CHAIR: That's not the feedback that a number of law enforcement agencies have put in their submissions, which are all publicly available for you to see. I would have thought that, if you're trying to avoid further regulations for tech companies, you would be keeping track of how often they're requested to assist law enforcement and whether or not they're providing that assistance quickly. Is that not a fair assumption?

Ms Gillespie-Jones: I'm happy to take on notice how often the request is being made. I think it's data that should be accessible. I don't have it at my fingertips.

Communications Alliance response

Our platform members transparently report on law enforcement requests they receive on their respective websites:

Facebook

Google

TikTok

Twitter

We note that response times for requests depend on a variety of factors including:

- whether the request has been correctly addressed;
- whether the request included all of the information that the provider needed to respond;
- whether the provider needed to revert with questions;
- the complexity of the request, i.e. the data that is being requested.

All providers have an emergency process for requesting information which is accessible at all times and, depending on the provider, yields a result within hours.

We also note that the response times that were cited in hearings relate to requests from law enforcement via the Mutual Legal Assistance Treaty (MLAT) process. Primarily, the delays are attributable to the complex and lengthy legal process involved and coordination between multiple government agencies via MLAT, rather than platforms' times to valid legal requests.

We anticipate that, once the Australia-US CLOUD Act agreement comes into effect, this should significantly shorten turnaround times for law enforcement requests.

2 QUESTION 2. Committee Hansard, p. 17

CHAIR:…Your submission says that, despite encryption: All of the existing cooperative processes will remain in place and will continue to provide meaningful data for law enforcement investigations. That statement contrasts with the evidence we're receiving from law enforcement agencies. The AFP itself is predicting that up to 60 per cent of its NCMEC referrals will be lost when Facebook goes to end-to-end encryption. Again, have your members looked at to what extent the movement to encryption will prevent self referrals from their platforms?

…

CHAIR: Do you not think it's reasonable, if companies move to encryption, given the seriousness of protecting kids, that they make some effort to quantify what the impact on discovering CAM material will be?

Ms Gillespie-Jones: It may be the case that they have quantified it. I'm not aware of a figure. I am happy to take that figure on notice too, or the question on notice.

Communications Alliance response

[We note that the AFP was quoting NCMEC which in turn claimed that 50% of Facebook's reports will be lost when Messenger moves to end-to-end encryption.]

The use of end-to-end encryption for private messaging does not prevent the ability of technology companies to provide significant numbers of actionable reports to law enforcement. End-to-end encryption is already the global industry standard for private messaging and it has not prohibited companies from providing reports of CSAM. For example, WhatsApp is already end-to-end encrypted and – in 2020 – they made 400,000 reports to the NCMEC.

Google notes that the number of reports made to NCMEC has increased by 22% from 2019 to 2020 (547,875 in 2020 compared with 449,283 in 2019).

We also urge the Committee and law enforcement agencies to be cautious about seeing high numbers of referrals as a measure of success. The number of NCMEC referrals does not tell the whole story. For example, when Meta analysed their existing referrals to NCMEC, they found that 90 per cent of referrals were the same or visually similar to previously reported content (source: https://about.fb.com/news/2021/02/preventing-childexploitation-on-our-apps/). Digital platforms are working on preventative measures to stop the harm occurring on their services in the first place. Successfully preventing the material will lead to numbers going down.

Digital platforms are continuing to innovate and work with law enforcement, including to improve the ability to generate actionable reports to NCMEC from non-content account signals. These steps are helping to develop approaches to detecting and combatting CSAM in ways that are end-to-end resilient.

3 QUESTION 3. Committee Hansard, p. 18

CHAIR: …Could you not say that any communications for a child between 13 and 18 is not encrypted and, therefore, if an adult starts engaging in a conversation with that 13- or 18-year-old, that conversation between an adult and a child is not encrypted?

Ms Gillespie-Jones: My understanding was that that was not possible. I believe that's what you heard earlier this morning too. My understanding from previous discussions was that that was not possible. Again, I'm happy to confirm that, but my understanding is that that was not possible.

Communications Alliance response

Most experts are of the view that enabling for the circumvention of encryption for any users can undermine the security of all users.

Encryption also offers benefits to children and we note UNICEF's view that children should be able to enjoy the benefits from encryption:

"End-to-end encryption is necessary to protect the privacy and security of all people using digital communication channels. This includes children, minority groups, dissidents and vulnerable communities. The UN Special Rapporteur on Freedom of Expression has referred to end-to-end encryption as "the most basic building block" for security on digital messaging apps. Encryption is also important for national security."

(Source: UNICEF, Encryption, Privacy and Children's Right to Protection from Harm, Daniel Kardefelt-Winther, Emma Day, Gabrielle Berman, Sabine K. Witting, and Anjan Bose on behalf of UNICEF's cross-divisional task force on child online protection Office of Research - Innocenti Working Paper WP-2020-14 | October 2020)

4 QUESTION 4. Committee Hansard, p. 19

CHAIR: …

One of the other issues that has been raised by witnesses is law enforcement officers in this space are struggling to receive enough training to keep up with the changes and advances in technology that move so fast. Your submission mentions that your members have programs in place to provide some training for law enforcement officers. I wonder if you could expand on that, specifically if you had any data around how many training sessions have been held in the last two years, the topics that they covered and how many law enforcement officers were included as part of that training?

Ms Gillespie-Jones: No, I don't have the data at hand. Again, I will take it on notice. We would also say if law enforcement feel that there is a gap in specific knowledge that they would address, I think all of our members would be most willing to specifically also address a gap in knowledge or in technology, experiences et cetera that they need. But I'm very happy to try to get you some data as to the last two years.

Communications Alliance response

In addition to dedicated reporting and intake channels, providers host regular training sessions for federal, state, and territory law enforcement and government agencies (proactively individually as well as through DIGI, and upon request), as well as provide detailed guides and resources that assist in lodging requests with the respective companies

It is worth noting that in the past two years, due to the COVID pandemic, (often upon LEA request) some trainings have been postponed or been transformed into written material.