Senate Estimates opening statement
October 2023

Thank you Chair, and Committee members for the opportunity to make a brief opening statement.

The past six months have been transformative for eSafety.
We exercised new regulatory powers under the Online Safety Act, registering six industry codes and taking further steps to require transparency in connection with the Basic Online Safety Expectations.

As a result, tech companies that operate in Australia have become more transparent and accountable for safety on their platforms, and will soon have mandatory measures in place.

In February, we sent legal notices to major tech companies such as Twitter (now X), Google, TikTok, Twitch, and Discord. We asked them for details on how they are tackling child sexual exploitation, sexual extortion, and child abuse livestreaming.

Last week, we published their responses, identifying key gaps and inconsistencies. In some cases, they're falling way short.

Online child sexual exploitation is a major concern. Tech companies have a moral obligation to protect kids from harm on their platforms.

We also had concerns with two companies' compliance with our regulatory notices. We gave Google a formal warning for giving some general answers to specific questions.

Twitter/X did not answer some questions accurately and left sections blank. We issued the company an infringement notice and a $610,500 fine because we do consider it important for companies to comply with their regulatory obligations and to deter recipients of our notices from taking a similar approach, avoiding the important goal of transparency.

Separately, in June, we also asked Twitter/X about its efforts to tackle online hate. We will provide a public report on its response – and responsiveness - in due course.

In June, we also announced our decision to register five online safety codes proposed by the online industry, decline two codes and reserve our decision on an eighth code. These codes were to address illegal content such as child sexual abuse material and pro-terror content across the technology ecosystem.

We determined that the two codes which were not registered, one for so-called "designated internet services" such as apps, websites, and storage services such as iCloud and OneDrive; and the other for "relevant electronic services" which includes dating sites, online games, and instant messaging, lacked sufficient safeguards for the community.

Consequently, we are working on mandatory industry standards for these areas, which will involve public consultation and will be tabled before Parliament in early 2024.

In September, we approved a revised online safety code for internet search engines. We had postponed registering this code because Google and Microsoft had plans to use generative AI in their search engines but this new functionality was not covered in the codes submitted to us.

The updated code now includes safeguards against the problems generative AI can create. It requires search engines such as Google, Bing, and Yahoo to actively reduce the risk of class 1 content, such as child sexual abuse material, in search results and prevent AI from generating fake versions of such content.

The creation and communication of so-called self-generated child sexual abuse material is a growing concern. Our study reviewed 1,330 URLs and found 12% of the material was self-generated. Also, 25% of the material came from family homes, some depicting children being ordered to undress and perform acts while their parents are in the next room.

Earlier, we also reported that cyberbullying complaints involving children under 14 had tripled since 2019, with May 2023 seeing the highest number of reports since the scheme's inception in 2015.

Our data shows that a rise in screen time following the pandemic has coincided with an increase in sophisticated cyberbullying tactics, including impersonation accounts, as well as the "phoenixing" of accounts. We received about 230 complaints in May alone, with 100 involving children aged eight to thirteen.

In August, we published a position statement on generative AI, offering safety interventions the industry could adopt immediately to enhance user safety and empowerment. We warned that AI-generated child sexual abuse material and deepfakes had already been reported to our investigators.

We also revealed we had received reports of students using this technology to create sexually explicit content to bully others, adding to the concerns about AI-generated child sexual abuse.

We also updated our 2019 position statement on End to End Encryption (E2EE), surfacing up industry best practice in finding and deploying proactive and systemic solutions to prevent and detect illegal content. We make clear that eSafety does not expect or desire companies to design systematic vulnerabilities or weaknesses into E2EE services, but nor does E2EE deployment absolve platforms and services of responsibility for hosting or facilitating the sharing of child sexual abuse material or terrorist content. Solutions are possible and evolving and we expect industry to mindfully design and balance the imperatives of safety, security and privacy.

We updated our Memorandum of Understanding to make sure our agreement with Queensland Police reflects our expanded role under the Online Safety Act and aids police officers in dealing with online harms.

Finally, over the fortnight, we have seen tragic events unfolding in the Middle East. eSafety is aware of concerns in the community about the spread of distressing and violent material from the Israel-Gaza conflict online.

eSafety has met with several online platforms to discuss their preparedness to protect Australians from such material. We will continue to engage with them to better understand what they are doing to enforce their terms of service and rapidly remove violent, harmful material.

As part of our ongoing work with Australian educators, eSafety has also issued online safety and reporting advice to Australian schools through the National Online Safety Education Council and eSafety Trusted Education Providers around how to prevent young people's exposure to distressing online content.

At the time of this statement, we have received a small number of reports of terrorist or extreme violent material related to this conflict. We have bolstered our response capacity and are ready -- through judicious use of our regulatory powers -- to support efforts to address an online crisis event, whatever the day or week, or time of day.

I must thank the dedicated eSafety team and our partners as we strive to make the online world safer for all Australians.

We appreciate your trust as we continue our crucial mission.

Thank you. I look forward to your questions.