What is a government's role in removing CSAM?

INHOPE SUMMIT

SLIDE 1 – OPENING SLIDE

Hello everyone!

I'd like to start by **thanking** all of the digital first responders here today. Being on the digital frontlines, seeing what you see and doing what you do can be hard and confronting work.

But it is **vital** work, and my gratitude and admiration go out to you all.

It is an honour to be speaking with you all today at the INHOPE Summit about the scourge of child sexual exploitation online, and the increasingly pivotal role being played by government bodies such as the Australian eSafety Commissioner.

I have been working at the intersection of technology policy, safety and social justice for the past 30 years – including more than 2 decades in the tech sector - so have witnessed the evolution and shift in methodologies of online predation over this period.

Never have I been more horrified at the scale and scope of this crime type, nor the extent of devastation it wreaks.

SLIDE 2 – PRIOR TO THE INTERNET

Prior to the Internet, the sexual abuse and exploitation of children were crimes of proximity: proximity to victims – whether intra-familial or deliberate positioning of access to children – AND proximity to other like-minded offenders with whom they shared material in hard copy format.

SLIDE 3 – LATE 1980S TO MID-1990S

From the late 1980s to mid-1990s, offenders turned to exchanging images online via clumsy, obscure bulletin boards, Usenet groups and email. The method of transmission was low-speed dial-up and images were often poor-resolution scans of CSEM magazines from the 1970s.

SLIDE 4 – 2000 ONWARDS

Since the turn of the Millennium, however, Moore's Law has been in full effect: network transmission, computation, digitisation, and image-processing technologies have achieved spectacular gains. While many of these gains bring myriad benefits, the Internet is now a highly enabling environment for the creation and distribution of CSEM images and videos. Through social media networks and integration of communications technologies, it also provides a vast new constellation of potential targets and victims for predators.

SLIDE 5 – Endless Victimisation & Re-Victimisation

Inconsistent laws and regulations, the tolerance of CSEM hosting in permissive jurisdictions, and a lack of overall global governance arrangements all support an environment where offenders can share and profit from the creation of CSEM, all

with little risk of detection – or penalty. This contributes to what sometimes appears to be the endless victimisation and re-victimisation of children and young people. A phenomenon my investigators – and many of you – witness every single day.

SLIDE 6 – Strengthened capabilities of authorities

There is an obverse to this: advanced technologies, capabilities, tools and skills have significantly lifted the capability of authorities combating CSEM. The better detection of child sexual exploitation material, disruption of offender communities, prosecution of offenders and interventions to rescue children have produced outstanding results. A recent example is the rescue of 14 children in the Philippines after Australian police identified a 68 year-old Victorian man involved in long-distance sexual exploitation.

This **is** an arms race, and I am very pleased to report that governments around the world are increasingly stepping up to address these challenges head on.

As Australia's online safety regulator, the protection of children online is my primary focus, and I would like to share with you some of the insights and lessons we have learned in the six years eSafety has been up and running.

SLIDE 7 – First Government Agency

Created in 2015, eSafety is the first government online safety regulator in the world whose sole purpose is the protection of its citizens online.

As the first regulator, there was no play book for preventing online harms, so we've had to fill in the pages as we've gone along.

We now believe we have developed a successful, practical and replicable model that focuses on three key areas - Protection, Prevention, and Proactive & Systematic change.

And it is protection where I'd like to begin because our regulatory schemes represent the tip of the spear in our fight to protect vulnerable children online.

SLIDE 8 - Protection

eSafety has a range of civil powers to compel takedown of illegal or harmful content, whether it's child sexual abuse material, pro-terrorist content, image-based abuse – or the non-consensual sharing of intimate images – and serious cyberbullying of a child.

But I think it's fair to say our priority as an agency, and the bulk of the work we do, is focused on the removal of child sexual exploitation material.

This important job falls to our eSafety Investigations team, who on a daily basis are exposed to some of the worst of humanity. Of course, some of the most distressing content involves child sexual abuse material, material that depicts the torture and abuse of innocent children for sexual gratification and profit.

However, we also respond to a growing number of reports from Australian young people about image-based abuse where images and videos showing them when under 18 are shared without their consent. Of course, in many cases, this too amounts to child sexual exploitation.

Sadly, my investigators are busier than ever.

SLIDE 9 - Covid-19 and the changing threat surface (multiple slides)

2020 was a year like no other and one I think most of us would probably rather forget. 2021 is starting to feel a bit like that for us here in Australia too – we in Sydney are now in our 13th week of our 5th lockdown!

The Covid-19 Pandemic has certainly seen the internet become an essential utility as the whole world turned to it to continue to work, learn, communicate and be entertained.

More of us began inhabiting the online world, and Australians were no exception. During the main COVID period of 2020, 60% made more video calls online with family and friends, and nearly 90% said the Internet was essential for at least one activity.

However, fuelled by fear uncertainty and doubt, many online harms became supercharged in ways we weren't entirely prepared for, and in Australia we saw spikes across all our reporting areas – and I think it is probably a universal truism that polarisation of debate online has further turned the online world into a toxic cesspool.

During 2020, Our Investigations team received **21,000** public reports of illegal and harmful content, the majority of which involved child sexual abuse material. This was the most in the scheme's 20-year history and a 90 per cent increase compared to 2019.

We also saw a **114%** increase in reports of image-based abuse – about a third of which related to under 18s.

SLIDE 10 - UNSW COVID-19 research findings

Our experiences during COVID-19 were consistently mirrored around the world. In research we funded by Drs. Michael Salter and Tim Wong from UNSW, many agencies, hotlines and police forces reported increases – some of them major – in child sexual abuse material, online grooming behaviour, online abuse communities, and online risk taking by minors during the 2020 COVID period.

There was evidence of more children being victimised online, with just over a third of agencies reporting a major increase in taking reports of online child abuse, and more than 60% reporting an increase in the investigations in this area.

Offenders were especially active. Almost a third of agencies reported a major increase in adults viewing CSEM, and more than 40% reported a major increase in adults sharing or distributing child sexual abuse material.

SLIDE 11 – What we are seeing

Sadly, these elevated levels of online abuse have shown no signs of abating in the first half of this year, and what we are seeing represents an alarming new normal, especially in the fight against the spread of child sexual exploitation material. Along with the elevated levels of online abuse – up an additional 30% in the first half of this

year – we have also seen some worrying new trends in how children are being exploited and abused online.

eSafety's research shows that Australian teens are exposed to a range of risks and threats online. More than 40% of young Internet users report negative experiences online. These include being contacted by a stranger (30%) and receiving inappropriate or unwanted content such as pornography (20%). While many teens take some form of action against the unwelcome contact, less than half mention it to family or friends (43%) or report it (40%).

SLIDE 12 – What we are seeing 2 – Coerced CSEM

Our investigators are also seeing higher volumes of **'coerced' child sexual exploitation material** where 6 or 7-year old children have been manipulated or intimidated into performing sex acts for the camera on iPhones or iPads in the "privacy" of their bedrooms and bathrooms.

In some of these cases, we have heard the voices of parents, unaware, in the next room.

About 25-30% of reports about image-based abuse are made by those aged under 18 years. Most under-18 reporters are aged between 13 and 17 years, with only a small percentage (7%) under 13. This form of abuse sometimes even escalates to physical meetings and contact offending. Almost all reports we receive concern some form of sexual exploitation or extortion: only 8% concern peer-group sharing of intimate imagery.

We work closely with our colleagues in law enforcement on these matters, especially through the AFP-led Australian Centre to Counter Child Exploitation.

SLIDE 13 - The new OSA reforms

And these growing threats have prompted the Australian Government to significantly bolster our protective powers with important reforms to Australia's Online Safety Act.

While countries around the world take their first tentative steps towards online regulation, Australia is already reforming and improving our framework around online safety regulation across a range of online harms.

This new Act builds upon the strengths of our existing legislative framework to provide eSafety with expanded powers to better protect all Australians across all platforms where this harm is occurring, including video gaming platforms, dating websites, and even encrypted private messaging apps.

For the first time anywhere in the world, eSafety will formally begin operating a new adult cyber abuse scheme to finally give Australian adults who are the victims of seriously harmful online abuse, somewhere to turn when the platforms fail to act.

And there will be significant financial penalties for perpetrators, so trolls will no longer feel safe to perpetuate abuse and online hate with impunity.

Added to this, the time platforms have to remove harmful content after receiving a notice from the eSafety Commissioner will be halved – from 48 hours to 24 – greatly reducing the mental and emotional distress experienced by survivors.

And importantly, our ability to fight the scourge of child sexual exploitation material online will be significantly boosted with the modernisation of our Online Content Scheme, giving eSafety the power to tackle this distressing content no matter where it is hosted.

The government is also lifting the bar on what it expects of the tech industry, setting out a core set of basic online safety expectations industry must uphold to improve and promote online safety if they wish to continue to operate in Australia.

The new Act will commence in January 2022, with new industry codes to be registered by July.

While a lot of changes are coming, one thing that will remain the same is eSafety's focus on providing a citizen-focused service to help keep all Australians safer online.

SLIDE 14- Prevention

While this important new legislation arms us with potent new weapons in the fight against all forms of online abuse, our primary goal at eSafety is to prevent the online harms we see every day from happening in the first place.

We are striving to achieve this through evidence-based research, education resources and community programs which are designed to target specific audiences giving people of all ages and backgrounds the right tools to protect themselves online.

We believe this a lifelong educational journey that should begin in the home as early as possible because we know **94% of 4-year-olds** in Australia have access to an internet connect device, **42% by the age of 2**.

I'm sure we'd all agree, that's pretty early!

And that's why for us it all begins with our Early Years program which reinforces the guiding principles for young children - to **be safe**, **be kind**, **be curious**, and to **ask for help** if something goes wrong online. We encourage parents to speak often to their children about what is happening online and to instil good digital hygiene practices and to encourage help-seeking behaviours early.

SLIDE 15 (four Rs of digital age)

Schools have a big role to play here, too.

While still an important cornerstone of education, the world has moved on from the traditional 3Rs of reading, (w)riting and (a)rithmetic. We must now also teach the four Rs of the digital age - **respect**, **resilience**, **responsibility** and **reasoning**.

Today's kids face challenges many of their parents never experienced like the pressures of social media, online bullying, dealing with unwanted messages or contact from strangers, pressures to engage in sexting, or just having to decide what news is real or fake.

We know fear-based messages don't work so we need to be reinforcing these important lessons in a positive, pragmatic and non-judgmental way.

We also need to reinforce similar messages to parents to be **aware** of the dangers without being **alarmed**. A key piece of advice we tell parents is to be present and to take an active interest in their children's online lives as they do their everyday lives.

As parents, we're good at asking our kids how their day was at school or if they scored any goals at soccer, but we're not so good at asking them about what's going on online. And that needs to become part of the standard dinner table conversation.

Our eSafety Guide was created to help parents demystify this online world that has now become such a huge part of their children's lives – and because it's online, all of these materials are available to anyone, anywhere at esafety.gov.au.

SLIDE 16 - Proactive change

But the responsibility for online safety cannot continue to fall solely on the shoulders of children and their often-overwhelmed parents, and this is where Proactive and Systemic change comes in.

We've all known the harms for over two decades and the tech companies are also well aware of how their platforms have been weaponised. Look no further than the Wall Street Journal Facebook Files & Instagram chronicles of last week. So, it is truly time for the entire industry to take responsibility for how their services are being used to harm children.

So how do we change the future?

SLIDE 17 - Safety by design (Pic of a car or crash test dummy)

At eSafety, we strongly believe the answer lies in something we call Safety by Design.

And, this is largely because the online world we inhabit now wasn't built for safety, it was built for speed. Few guardrails have been erected on these digital roadways, and no virtual seatbelts have been deployed at the outset to prevent our children from reaching the darkest recesses of the web.

When get into our cars today, we take for granted that the brakes will work and the air bags will deploy. We trust that the protections built into our cars, guided by international standards, will keep us safer on the road. Safety is built in, by design.

Shouldn't we all expect the same standards of technology companies as we, and our children, navigate the internet? We believe we should.

We have spent the past three years working with big tech to lead them down a path that will fundamentally change how they design, develop and deploy their products, with safety at the core.

After consultation with more than 180 organisations around the world, we recently launched our world-first, free, interactive assessment tools for companies of all sizes and levels of maturity so that they can assess and mitigate their safety risks. The tools provide targeted best practice guidance, and it is our belief that we can begin to lift safety standards across the tech industry.

SLIDE 18 - Safety by Design Assessment Tool

While the sheer magnitude of these threats can feel overwhelming, we strongly believe that many of the harms can be engineered out with some additional foresight.

That's why we have created eSafety's Safety by Design framework: a set of principles that industry can use to design stronger, more resilient systems and products that prioritise user safety from the first byte of code.

The initiative has been developed with industry for industry. It recognises that, if we wish to end online child sexual exploitation and abuse, industry needs to be at the heart of any process to effect cultural change through enhanced leadership in the area of online safety – bringing this focus closer into line with longstanding commitments to security and privacy.

Safety by Design has three main pillars: platform responsibility, user empowerment and autonomy, and transparency and accountability. These voluntary interactive tools reflect these pillars and enable companies – from start-ups to major enterprises – to evaluate the safety of their systems, processes and practices and produces a targeted report to help them identify and plug these shortcomings.

Online safety needs are far reaching so we're also working to embed safety by design into interdisciplinary curricula across the university sector so that the next generation of computer scientists and engineers are learning to code with conscience.

The VC and investment community also have a critical role to play here in stewarding more responsible development processes in the start-up sector. We will also be continuing our work with the banking and financial sector, which is combatting a proliferation of micro-aggressions in online payment transactions but also unwittingly funding child sexual abuse enterprises, including the paid live streaming of online abuse. We've already seen the impact credit card and payment system vendors can have in enforcing better safety standards – look no further than recent efforts to purge CSEM and IBA from Pornhub and to enforce higher standards at OnlyFans.

In short, there is much work to do here and we welcome your engagement!

SLIDE 19 – Challenges now and into the future

Another way eSafety seeks to stay ahead of the curve to ensure our content and programs reflect current information, technological developments and global trends, we continually scan for new research, policy, legislative and technical updates and cross-reference with our investigative insights.

We developed our first tech trends and challenges brief on the weaponisation of deepfakes 18 months ago – and we could not get mainstream media interest at the time. Now, it's difficult to see a technology rag that doesn't have some mention of the horrors wrought on humanity by deepfakes, GANs, AI or algorithms. So, we learned that the right timing and balance was important, particularly when weighing positive use cases against potential risks.

You'll see everything from anonymity and identity shielding, to the potential of "rape by default" in the metaverse, trends around sexual extortion and our most recent

brief on decentralisation where we believe that we need to be looking critically at internet governance models of the Web 3.0 world now to ensure that privacy, safety and security essentials are baked in and that there are still ways to remediate online harms.

SLIDE 20 - Working with our international partners

Of course, none of our organisations or even sectors exist in a vacuum. We are part of an incredibly complex global ecosystem.

As a government entity whose laws are national – with some extraterritorial reach – eSafety understands that our success hinges upon robust, global partnerships. These international alliances will become more important than ever in helping us identify victims and disrupt the trade in this distressing material.

As a member of INHOPE, we contribute to the rapid take-down of CSAM, and actively participate in both the governance and operation of the organisation and network.

It is incredible that INHOPE exchanged reports about more than one million URLs depicting suspected CSEM last year alone. More than 90 percent of the content showed the abuse and exploitation of girls, and just over three quarters of all reported CSEM involved the abuse or exploitation of pre-pubescent children.

We often say in our circles that it takes a network to disrupt a network and INHOPE is a critical player and facilitator in this sphere that makes the rapid removal of this abhorrent content possible.

SLIDE 21 – Other partnerships

Whilst the security, privacy and digital rights communities have had long established alliances over the decades, online safety and child protection organisations are developing burgeoning strength. We at eSafety work closely with our local law enforcement partners at the state and federal level but we are also a member of the Child Dignity Alliance and on the Board of the WEPROTECT Global Alliance, which now has 100 countries and 70 companies committed to making significant steps towards the eradication of child sexual exploitation. ESafety is also proud to have our head of investigations, Toby Dagg, serving as Vice President of the INHOPE Board.

These international partnerships are vital, but the world needs to go further, with countries adopting a truly coordinated approach – across sectors, borders and transcending language, culture & faith.

SLIDE 22 - We are not alone

After 6 years of online safety regulation, we now actually deal with very little CSAM that is hosted in Australia. In fact, we are almost exclusively dealing with content that is hosted overseas.

While this shows our efforts are having a real impact on our own shores, when it comes to more permissive online hosting environments overseas, our actions are limited by sovereignty and jurisdiction.

But things are changing. Ireland has announced the establishment of its own Online Safety Commissioner and Fiji has already established theirs. The UK is bolstering OFCOM to tackle online harms and we've had a number of conversations with

Canada, the EU and across Asia Pacific about setting up their own national online safety regulators. We hope the U.S. and others join us too – and the global network we hope to build of like-minded agencies.

I suspect that in the next **5-10 years** we will see an international network of online safety regulators working together to tighten the circle around those who trade in and profit from this distressing material.

SLIDE 23 – Multi-layered Approach to Protecting Children

We look forward to other regulators coming on-board and I believe we will need them to if we are going to really tackle an almost universal range of online harms. We are openly sharing our learnings and will be looking to foster a consistent global regulatory framework for online harms so that we don't move towards a global regulatory Splinternet – which would be difficult, if not impossible, for industry to adhere to.

As I said at the start, I think we've found a formula that helps address online safety issues from three distinct axes – protection, prevention and proactive change – that can genuinely provide protections for our citizens whilst shifting responsibility to where it needs to sit.

There's no question we've reached that tipping point where unrestrained proliferation of technology without regulatory guardrails is causing harm to individuals and institutions and some would say, is tearing at the fabric of democracy and civilised society.

That old adage that, "You cannot hope to fix a problem unless you are first willing to acknowledge you have one," truly resonates in this context.

And Houston, I think we have a problem here...

SLIDE 24 – Balancing Fundamental Rights

There is no question that Big tech has some big challenges to surmount. I believe one of their primary ones is making sure that they strike the right balance between a range of fundamental human rights. We at eSafety see countless examples everyday of unfettered freedom of expression veering headlong into the lane of targeted misogynistic, hateful and racial harassment – actually shutting down the purported speech of vulnerable communities and voices we're trying to protect.

Shouldn't users also have the right to be online without the fear or threat of online violence?

And why is it that the fundamental rights of a child and the right to human dignity when it comes to the proliferation of child sexual abuse material have effectively been subjugated to privacy and data protection?

We saw this tension with the ePrivacy derogation earlier in the year and again in the five weeks following Apple's announcement of their plans to roll out technologies to detect known child sexual abuse imagery hosted on their platforms, which has now been halted "for an indefinite period," which many of us believe creates a concerning precedent.

SLIDE 25 – NCMEC Reports

If you take a look at these 2019 and 2020 NCMEC reporting numbers of the major technology players, you see some huge disparities here. You see very clearly how Apple and Amazon were so clearly behind their industry peers in scanning for and detecting CSAM on their services – Amazon saw a modest uplift in their numbers in 2020 with the inclusion of Twitch data.

While I think we could take issue with Apple's approach to rolling out – and then pulling, these tools – without bringing the child protection sector along – and some of us may even take issue with the technological approach, I think so many pundits missed the big picture here.

This attempt at finding a middle ground was Apple acknowledging that there was indeed a problem. It was also an acknowledgement that they were lagging behind their industry peers and were ultimately NOT taking responsibly for the child abuse material on their services. Can anyone credibly believe with over 1 billion Apple handsets in circulation and close to a billion iCloud users, that there were only 205 instances of CSAM on their services versus Facebook's 15.9 million? Or that this unlikely total only increased by 65 in 2020?

Why is this an issue that we cannot seem to find a compromise on? After all, our devices and online services run spam filters, and are routinely scanned for malware and viruses and yet we don't see the same uproar from the techno-libertarian sector.

Online services will readily take down content that violates intellectual property but won't do the same for images of children being raped and tortured?

Clearly, we need to find common ground and SUPPORT companies to achieve this balance, but more importantly, we need to do the right thing.

Slide 26 - Conclusion

And that is precisely what this Summit is all about. Working together to fight a common enemy – those offenders that seek to prey upon children and who can now share and profit from the creation of CSEM – all with little risk of detection or punishment.

These are the same perpetrators who exploit inconsistent laws and permissive hosting environments, misuse technology for their own ends and weaponise online platforms, harming users and undermining consumer trust in the high-tech sector.

These offenders are visible to the collective eyes of industry, government and the advocacy community. This is precisely why we need to forge cross-sectoral consensus and ensure that we are successful in achieving this great balancing act – where security is bolstered, privacy is preserved, and online safety is more than a mere afterthought.

Thank you.