

Keeping Australians safer online



About eSafety

Education and prevention



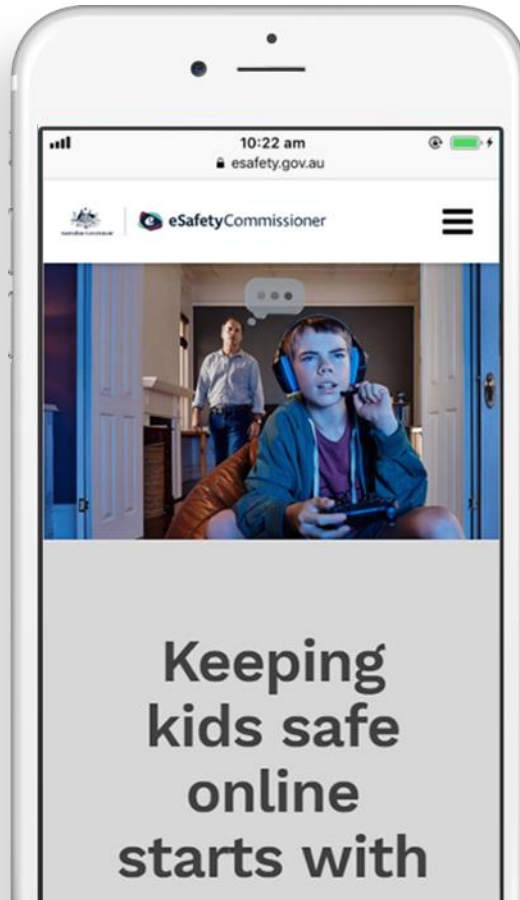
Research and
evaluation



Evidenced based
resources



Training – webinars
and face to face



Investigation and removal



Serious cyberbullying
material



Illegal online
content



Image-based
abuse

Cyberreport

Investigates complaints
from Australian residents
and law enforcement

Prioritises serious
content such as:



Offensive
and illegal
online
content

and



Child sexual
abuse
material



Pro-terrorist
content



Content that
promotes, incites
or instructs in
crime or violence



Abhorrent
violent
material

Cloudflare protocol

Of equal concern to me is the use of Cloudflare by websites hosting far-right and extremist content. In the immediate wake of the Christchurch attacks the eSafety Commissioner, along with other Australian government agencies, saw a rapid proliferation of the attack video and associated manifesto across sites such as Kiwi farm, 8Chan Bit Chute – all of which are protected by Cloudflare.



Dear Cloudflare,

I am Australia's eSafety Commissioner, charged with regulating and promoting online safety for Australians. My role includes the regulation of online content under Schedules 5 and 7 to the *Broadcasting Services Act 1992* (Cth) ('the Online Content Scheme').

The Online Content Scheme empowers me to investigate illegal online content such as child sexual abuse material (CSAM) and content advocating terrorism. Where such content is hosted in Australia, I may issue legally-enforceable takedown notices to content hosts.

We have observed that a large and increasing number of our investigations involve Cloudflare. Clearly, the use of a reverse-proxy server by sites hosting illegal web content increases the complexity of host tracing. This makes it difficult – and in some cases, impossible – to determine whether there is an Australian connection to prohibited material or whether it is hosted overseas.

We have been advised in prior correspondence with you in March, 2018 to forward requests for information about the true IP address through your online reporting form at <https://www.cloudflare.com/abuse/>.

However, I am advised that it is not uncommon for these enquiries to go unanswered, even in the case of child sexual abuse material. As an alternative, we have tried making requests to abuseteam@cloudflare.com and the generic abuse@cloudflare.com address and have found inconsistent results provided. When they are returned, key information is often missing, such as your reason for being unable to provide an IP address.

Some examples:

- On 11 March 2019, Cyber Report requested hosting information in connection with content on the amateurlr.com domain that showed contact sexual abuse of a child. There has been no response.
- On 21 March 2019, Cyber Report requested hosting information in connection with content on the cajadinamica.info domain showing images of child sexual exploitation. There has been no response.
- On 31 January 2019, Cyber Report emailed requests for information about 12 URLs hosting CSAM. There was no reply. Our investigator then individually entered all 12 URLs into the webform provided at <https://www.cloudflare.com/abuse/>. Of the 12, only four responses were supplied by Cloudflare.
- On 19 December 2018, Cyber Report sent three requests to Cloudflare about child sexual abuse and exploitation material provided via the maxcuties.fun, myuenozra.site and bamynn.site domains. We received no response.

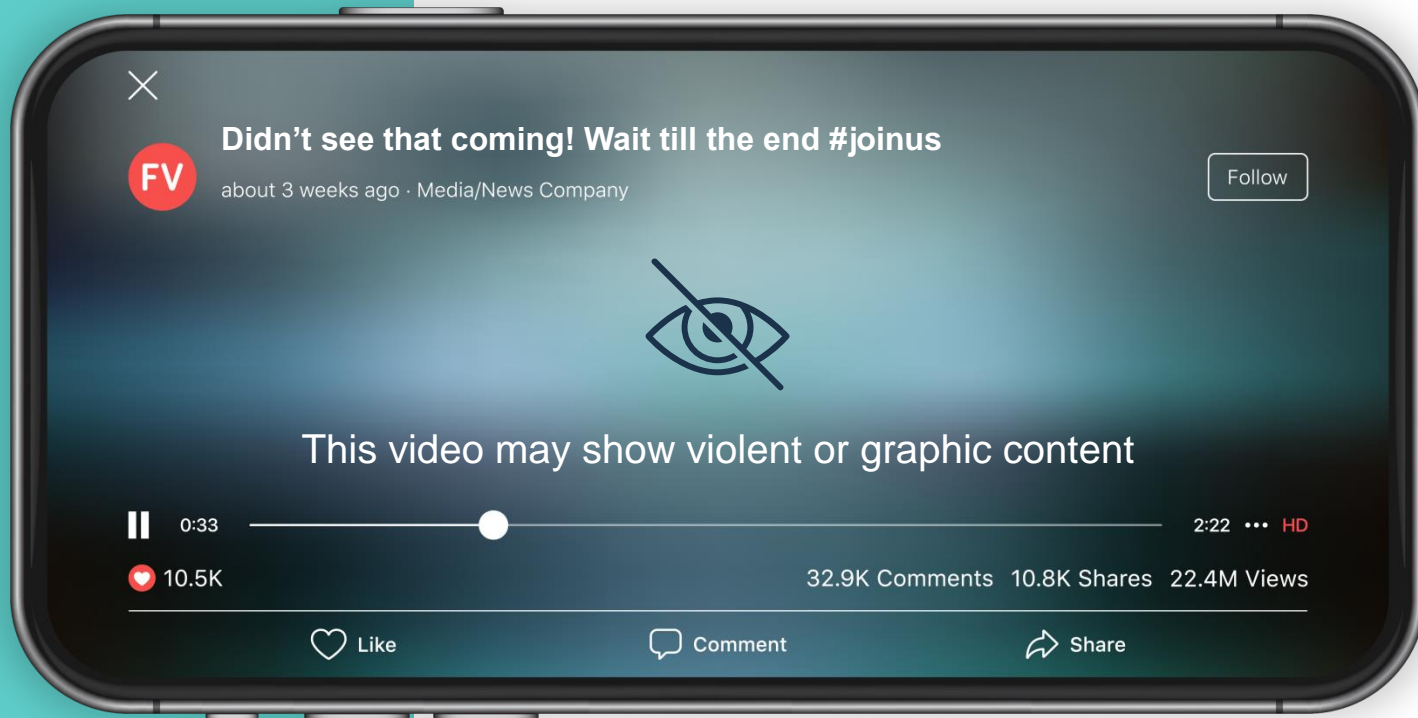
Of equal concern to me is the use of Cloudflare by websites hosting far-right and extremist content. In the immediate wake of the Christchurch attacks the eSafety Commissioner, along with other Australian government agencies, saw a rapid proliferation of the attack video and associated manifesto across sites such as Kiwifarms, 8Chan and BitChute - all of which are protected by Cloudflare.

P: 1800 880 176

E: first.surname@esafety.gov.au

esafety.gov.au

Abhorrent Violent Material legislation





Taskforce recommendations



Facebook



Instagram



LinkedIn



Twitter



OPTUS



Child sexual abuse
material shared by

750,000

users across the internet



INHOPE received

1.2 million

reports of child sexual
abuse material

Parents



81%

are giving their
pre-schoolers
access to the
internet



3 in 4

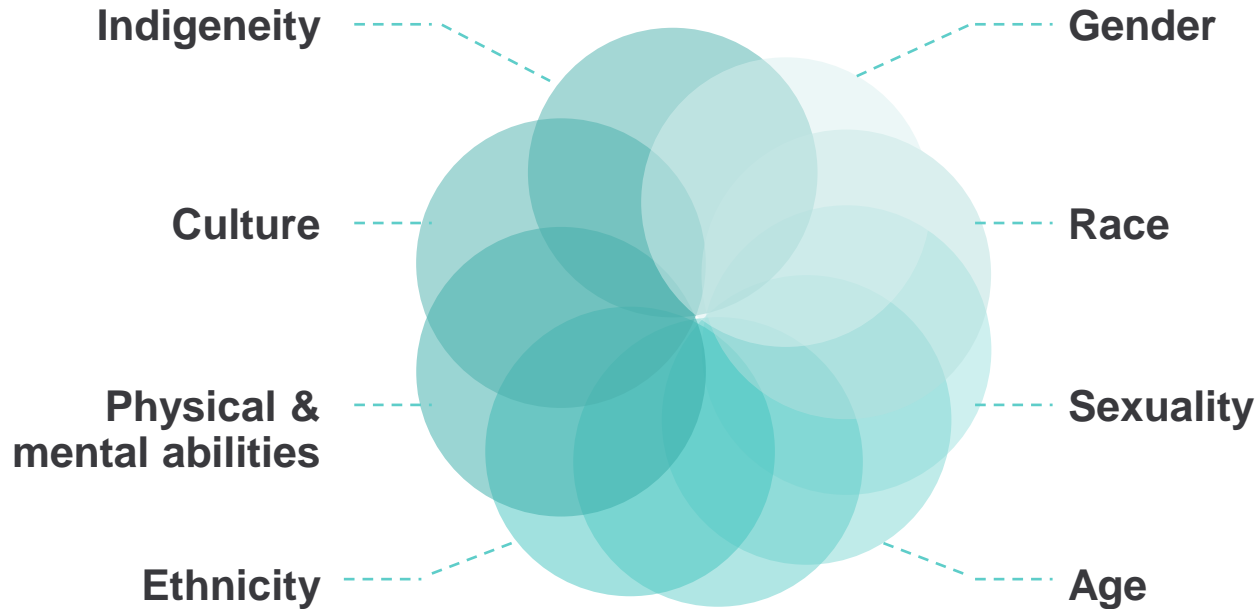
parents took some
form of action to
try and keep their
child safe online



<50%

of parents felt
confident dealing
with serious
online issues

Intersectionality



We take an inclusive and strengths-based approach

Reducing Impact on Victims



Behind each image is a child being harmed and abused

Strategic Goal



Proactive change

eSafety draws on its expertise, complaint trends and research to drive long-term, systemic change for measurable impact and improvement in the online environment

Our Proactive Change Tactics

Work across sectors, including directly with **industry**, to develop principles for making platforms safer at the outset through initiatives like Safety by Design.

Employ sophisticated **investigative strategies** to disrupt the proliferation of child sexual abuse material.

Identify emerging **issues, technologies** and trends to ensure agility in responding to these developments and in anticipating their potential misuse.



Invest in **technologies**, tools and partnerships to scale our reach and enhance our impact on the global stage.

Develop **evidence-based policy positions** and regulatory interventions on emerging issues and contribute to public debate, law reform and global thought leadership.

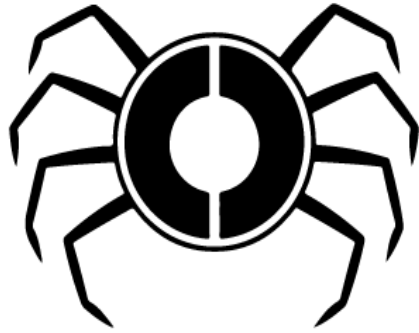
Looking to the future



**Strategic
approaches
through to
2022**

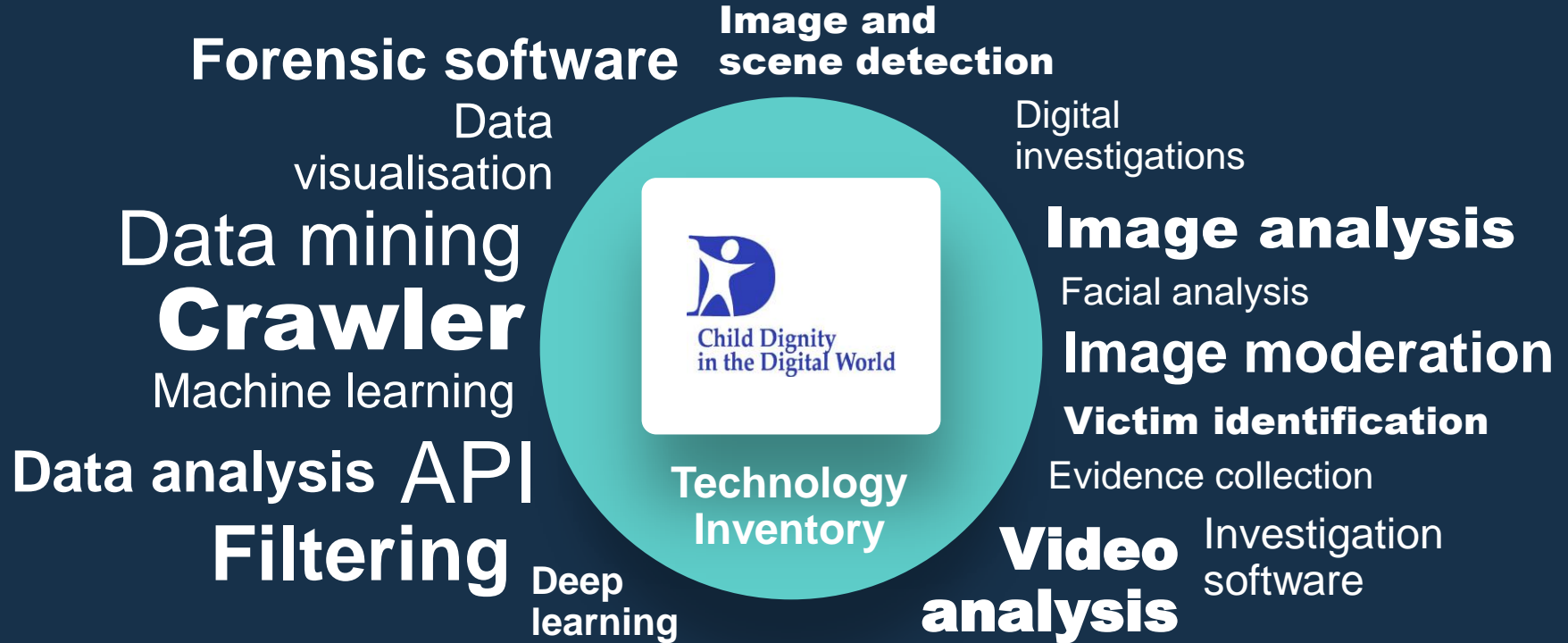


Project Arachnid



Project
Arachnid







Safety by Design

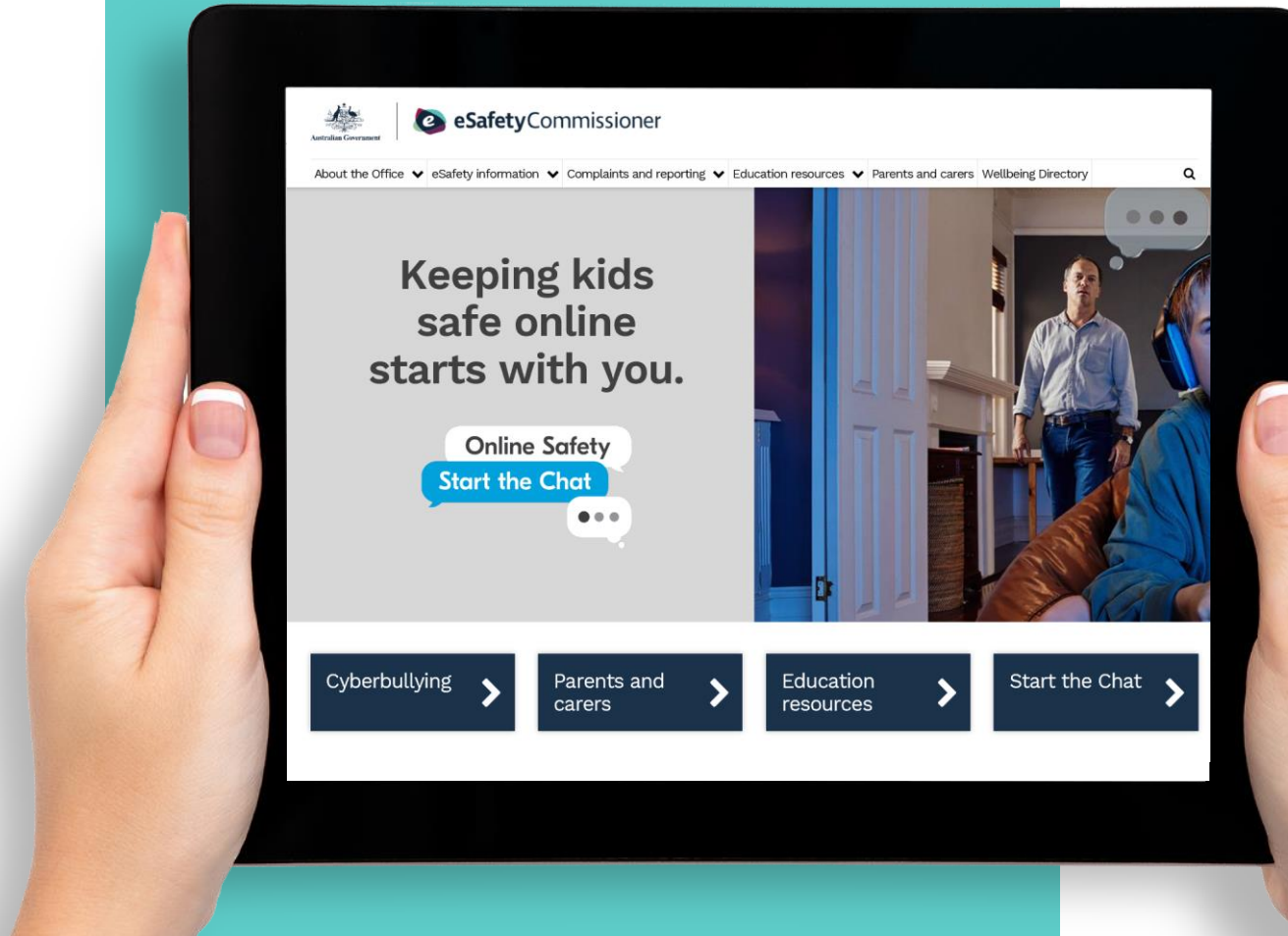


Consulted with industry, service providers, parents and carers and young people



Safety by design principles – underpinned by human rights standards

Let's work
together for a
better internet



eSafety Conference

11-12 September 2019 Sydney

8:45 - 9:30	KEYNOTE	Rights and resilience in the digital world Sonia Livingstone OBE	New findings on children's online risks and opportunities are informing improvements in policy and practice around the world. Is this enough to ensure children's rights and resilience in a digital world?	BALLROOM LVL 03
9:35 - 10:20	PANEL	Social media: negotiating the highs and lows Dr Amanda Third Professor Bronwyn Carlson Jocelyn Brewer	How does social media impact young people's wellbeing? Explore how the benefits of social media can be utilised to shape positive behaviour, while minimising risk.	BALLROOM LVL 03
10:25 - 11:10	KEYNOTE	The future of internet safety education. What works, what doesn't? David Finkelhor	Prevention programs do generally improve child safety. But Internet safety education still has a way to go. In adopting evidence-based techniques, targeting factors that are related to risk, and proving it can work.	BALLROOM LVL 03
11:10 - 11:30		Morning Tea		
11:35 - 12:15	KEYNOTE	Youth changing the world Tessy Ojo		BALLROOM LVL 03

 **eSafety¹⁹**
THE ONLINE
WORLD WE WANT

Thank you



eSafety Commissioner

esafety.gov.au