Australian Government

eSafetyCommissioner

Monday 23 August 2021

Ms Rosemary Sinclair AM
CEO
auDA
By email: consultation@aud.org.au

Dear Ms Sinclair

Thank you for the opportunity to provide feedback on auDA's proposed strategy for 2021 – 2025. I am encouraged by the proposal, which firmly cements auDA as a global leader in the management of trusted domain spaces, while also advocating for a free, secure and global Internet.

In preparing this submission, we have focused on questions 2 and 3 of the Consultation Paper.

The eSafety Commissioner

The eSafety Commissioner (eSafety) is Australia's national independent regulator for online safety. Our core objective is to minimise harm to Australians online.

eSafety is the first government agency in the world dedicated specifically to online safety. We lead, coordinate, educate and advise on online safety issues and aim to empower all Australians to have safer, more positive online experiences. One area of focus is on regulating various online harms.

When eSafety was formed in July 2015 (as the Children's eSafety Commissioner), a primary function involved administering a new regulatory scheme in relation to serious child cyberbullying. eSafety also assumed responsibility for the Online Content Scheme set out in Schedules 5 and 7 to the Broadcasting Services Act 1992 (Cth), and previously administered by the Australian Communications and Media Authority. Through the Online Content Scheme, eSafety prioritises reports about child sexual exploitation material (CSEM) and pro-terror content. We are a leading member of INHOPE,[1] with 95% of all CSEM we investigate notified to INHOPE members for removal in the host jurisdiction.

[1] The International Association of Internet Hotlines (INHOPE) is a membership organisation consisting of 46 anti-CSEM hotlines around the world. Members include the US National Centre for Missing and Exploited Children (NCMEC), the UK's Internet Watch Foundation (IWF), and France's Point de Contact. INHOPE's vision is an Internet free from child sexual abuse material, and the association works closely with domestic, international and European law enforcement (including INTERPOL and EUROPOL) to share intelligence and contribute to victim identification efforts. INHOPE was formed in 1999, and the Australian Government has been a member (first through the Australian Broadcasting Authority, then the Australian Communications and Media

Since then, eSafety's functions have broadened to include administration of a civil penalties regime in relation to image-based abuse ('IBA', sometimes incorrectly referred to as 'revenge porn'), the power to issue notices to content and hosting services about abhorrent violent material, and a function related to blocking websites providing access to certain terrorist content during an online crisis event.

There will soon be further changes to eSafety's powers, with the Online Safety Act 2021 (Cth) ('OSA') due to commence in January 2022. Through the OSA, eSafety's existing regulatory functions will be bolstered by a new scheme to tackle adult cyber abuse, and the power to require transparency reports from digital services through a set of Basic Online Safety Expectations. We have prepared a fact sheet on the OSA, which can be accessed here.

Strategic environment and opportunities

As noted in the Consultation Paper, COVID-19 has been a catalyst for significant digital transformation in Australia. Our own research has shown that, through the main COVID period of 2020, there was a substantial rise in the percentage of Australians using the Internet for activities such as keeping up to date with news, for entertainment, to keep in touch with friends and family and, unsurprisingly, work. Overwhelmingly, Australians view the Internet as an essential technology, with 86% seeing it as a 'good thing'.[2]

However, eSafety does see a range of harmful and negative dimensions to the Internet through our research and regulatory reporting schemes. Four in ten Australian adults report having a negative experience online. These include receiving unwanted messages, being sent inappropriate content, and having things said online to provoke an argument.[3] The number is slightly higher for younger Australians, who predominantly report unwanted contact, and unwanted or inappropriate content as sources of concern.[4]

Our harmful and illegal content reporting schemes saw an unprecedented increase in the number of reports from Australians made to eSafety during the 2020 COVID period. Overall, when 2020 is compared with 2019, reports about CSEM were 90% higher, while complaints about image-based abuse climbed by almost 115%. Cyberbullying and adult cyber abuse also intensified over the period, with reports increasing by 30% and 40%, respectively.

Authority, now the eSafety Commissioner) since 2000. Members include industry associations, charities and public authorities (including the eSafety Commissioner and the Korean Communications Standards Commission).

[2] eSafety Commissioner, 'COVID-19: impact on Australian adults' online activities and attitudes' (June 2020) <https://www.esafety.gov.au/sites/default/files/2020-06/Covid-19-impact-on-Australian-adults-online-report.pdf>, 3.

[3] Ibid.

[4] eSafety Commissioner, The digital lives of Aussie teens, <https://www.esafety.gov.au/sites/default/files/2021-02/The%20digital%20lives%20of%20Aussie%20teens.pdf>, 5.

This underscores the observation made in the Consultation Paper about heightened risks of harm through changes to the strategic environment. We agree and think that recognising the importance of online safety is an important corollary to efforts being made to bolster cyber security. While there are important differences in the tools and policies relevant to managing online safety and security risks, they are intrinsically related concepts. All those who play a role in maintaining and administering the Internet's critical infrastructure also have a part to play in driving up standards across both areas.

We agree with auDA's proposed vision and would add that unlocking positive social and economic value for Australians also requires a *safe* Internet.

Along with others such as the UK's Internet Watch Foundation (our sister hotline in the INHOPE network), we are deeply concerned about the continued misuse of certain country-code TLDs and generic TLDs by those distributing CSEM. auDA's leadership and maintenance of world-class standards have prevented the .au domain space from being abused for this and related purposes – an outcome for which we are thankful. Most CSEM websites are hosted via .com and .net domains, with the IWF recently calculating that they represent 82% of domains supporting CSEM.[5] Closer to home, we note that the .cc country-code TLD has been consistently abused for this purpose, appearing in the top ten most abuse TLD in the IWF's 2019 annual report.[6]

eSafety understands that auDA has no specific role in administering these domains. However, auDA is in a unique position through its management of the .au domain space to assist us in promoting online safety. In particular, we would call on auDA to use its reach and influence to drive up standards among ICANN members and registrars in relation to TLD abuse that supports the destructive and insidious online CSEM economy. The proposed strategy for 2021 – 2025 does not specifically address auDA's role as a source of positive influence to strengthen norms online and strengthen the governance of problematic TLDs. eSafety recommends that it should.

Safety by Design

One option auDA may wish to consider when finalising the strategy is eSafety's Safety by Design initiative.

Safety by Design has been developed with industry for industry. It recognises that, if we wish to end child sexual exploitation and abuse, industry needs to be at the heart of any process to effect cultural change through enhanced corporate social responsibility. eSafety has undertaken

[5] Internet Watch Foundation, *Annual Report 2020*, <https://www.iwf.org.uk/sites/default/files/inline-files/PDF%20of%20IWF%20Annual%20Report%202020%20FINAL%20reduced%20file%20size.pdf>, 69.

[6] Internet Watch Foundation, *Annual Report 2019,* <https://www.iwf.org.uk/sites/default/files/reports/2020-04/IWF_Annual_Report_2020_Low-res-Digital_AW_6mb.pdf>, 50.

extensive consultation with industry, civil society organisations, advocates, parents and young people themselves to understand how online harms develop and are experienced across broad and intersectional communities.

The principles underpinning Safety by Design have now been translated into a set of comprehensive assessment tools allowing companies – from start-ups to established enterprises – to evaluate the safety of their systems, processes and practices. This includes advising industry on how to ensure that robust moderation of conduct and content is possible before releasing products to the market, as well as how to authenticate users and prevent known techniques used by perpetrators to target and abuse others.

Safety by Design encourages technology companies, and indeed the broader technology industry, to help end child sexual exploitation and abuse by enhancing their corporate social responsibility. In part, this can be done by highlighting the innovation that is already occurring within the sector as well as encouraging technology companies to foster a global community and to be open in sharing their solutions.

User-centred design with consideration of children and young people is critical. Key touchpoints for industry consideration include implementing default privacy and safety settings at the highest possible levels, incorporating conversation controls and discoverable and seamless reporting pathways. Such measures proactively address the potential for online harm, while empowering users to regulate their own online experiences.

eSafety continues to work closely with industry to further implement existing safety measures, standards, requirements and guidance – as well as encourage them to innovate and transform the safety landscape further. Our forward workplan for Safety by Design includes working with the investment community to incorporate the principles into responsible investment practices; generating practical engagement with the assessment tools within the start-up community; focusing on marginalised and at-risk groups to ensure their needs are considered; and developing targeted resources for new and emerging sectors.

We think that applying a Safety by Design lens to auDA's proposed 2021 – 2025 strategy will enhance its outcomes.

The Web 3.0 Infrastructure

eSafety is actively thinking about how we might work with leaders such as auDA to help shape the future Web 3.0 infrastructure, with Safety by Design principles in mind.

In particular, we have been thinking deeply about decentralisation of the Internet. As you would know, the vision for decentralisation involves distributing control of data, and of user interactions and experiences. Decentralised networks are not reliant on a concentration of large technology companies maintaining server and storage infrastructure to operate.

While decentralisation can allow users to protect their information and control their online experiences, it can also make it more difficult to hold users (or the entities behind them) responsible for illegal and harmful content and conduct. The lack of a central authority, along with the storage and distribution of data across machines and jurisdictions, makes it difficult to moderate, regulate, and remove illegal and harmful content. For these reasons, there are concerns that a decentralised Internet may become a haven for CSEM and for users who have been removed from mainstream services and platforms.

Interest is growing in the tech community to develop the ‘DWeb’ and ‘DApps’. As mainstream platforms increasingly respond to and address CSEM on their services, the perceived impenetrability and unaccountability of decentralised environments could incentivise efforts to evade detection, to further create and distribute CSEM.

We must work collectively and across borders to encourage greater consistency and shared approaches to help counter online risks and harms on decentralised services and platforms. There is also a need to ensure that Safety by Design is given the same priority as Security and Privacy-by-Design in the design and development of decentralised services and in the broader Web 3.0 infrastructure.

Multi-stakeholder engagement

eSafety believes that strategies aimed at tackling harms online can only succeed through strong and effective engagement with a variety of stakeholders. We support this aspect of the proposed strategy, in particular its focus on community-led policy making.

eSafety is excited by auDA’s vision for the future and we hope our comments will assist you in your important work.

We look forward to being an active stakeholder going forward and wish you all the best in finalising a strategy that works to keep Australians both secure and safe online.

Should your team wish to discuss this submission, please contact **Mr Ross Anderson** at ross.anderson@esafety.gov.au or 02 9334 7747.

Yours sincerely,

Julie Inman Grant

Julie Inman Grant
eSafety Commissioner