



Inquiry into racism, hate and violence directed at Aboriginal and Torres Strait Islander peoples

Joint Standing Committee on Aboriginal and
Torres Strait Islander Affairs

May 2026

Contents

Introduction2

eSafety’s role and functions2

 Prevention.....3

 Protection3

 Proactive and systemic change3

Statutory review of the Online Safety Act3

Online hate4

Response to Terms of Reference4

 The nature, prevalence and impact of racism, hate and violence towards First Nations people, including trends over time 4

 The effect of online platforms on the reach, prominence and harm caused by racism and hate directed at First Nations people..... 6

 Initiatives that are effective in combating racism targeted at First Nations people and reduce individual and collective harm 8

 The threat posed by ideologically motivated extremism towards First Nations people and the role of intelligence and law enforcement agencies in protecting the community from that threat..... 12

 The effectiveness of avenues for reporting and responding to racism against Aboriginal and Torres Strait Islander people, including the consistency, timeliness and appropriateness of outcomes across jurisdictions and institutions 13

Conclusion..... 15

Introduction

The eSafety Commissioner (eSafety) welcomes the opportunity to make a submission to the Joint Standing Committee on Aboriginal and Torres Strait Islander Affairs' inquiry into racism, hate and violence directed at Aboriginal and Torres Strait Islander peoples.

Aboriginal and Torres Strait Islander peoples use technology and social media in ways that differ across cultural and language groups, and across urban, regional and remote communities. In addition to everyday communication, social media and online communication are used to maintain connections to community and share cultural knowledges and practices.

eSafety shares the Committee's concerns about racism, hate and violence experienced by First Nations people. We recognise that online hate can negatively impact a person's mental health, general wellbeing, and online engagement. It can also lead to harassment and physical violence offline and contribute to broader social harms. We also recognise that Aboriginal and Torres Strait Islander communities experience online hate at disproportionate rates when compared to the general Australian population.¹

In accordance with eSafety's role as Australia's online safety regulator, our submission will focus on hate that takes place online.

eSafety considers that an inclusive and holistic approach that addresses all forms of online hate, including online hate directed at Aboriginal and Torres Strait Islander peoples, and that promotes and requires systemic industry accountability is best capable of effectively and meaningfully addressing online hate in all forms.

To contextualise our submission, we will first provide an overview of eSafety's remit, role and approach in general terms, before addressing the Terms of Reference directly.

eSafety's role and functions

eSafety is Australia's independent regulator, educator and coordinator for online safety. Our purpose is to help safeguard Australians from online harms and to promote safer, more positive online experiences.

The eSafety Commissioner is an independent statutory office holder appointed by the Minister for Communications. The *Online Safety Act 2021* (Online Safety Act) sets out our legislative functions. Our regulatory approach is underpinned by three pillars: prevention, protection, and proactive and systemic change.

¹ eSafety Commissioner. (2025). *Fighting the tide: Encounters with online hate among targeted groups*. Australian Government. https://www.esafety.gov.au/sites/default/files/2025-02/Online-hate-report_Main-Feb25.pdf?v=1775691797629

Prevention

Through our research, education and training programs, we aim to build the capacity of Australians to interact safely online and to know where to seek help if issues arise. We do this by raising public awareness about online safety issues, risk prevention, and support pathways. We empower individuals and communities through training and education and produce free, evidence based, easy-to-use information and advice. To support these activities, we conduct research into online experiences and attitudes, and evaluate the effectiveness of safety interventions.

Protection

Where online harm does occur, eSafety offers tangible, rapid assistance. eSafety has powers to protect Australians on online services and platforms, via our complaints reporting schemes relating to four types of harm: cyberbullying of children, cyber abuse of adults, the non-consensual sharing of intimate images, and illegal or restricted online content.

Proactive and systemic change

With the rapid evolution of technology, eSafety knows we need to be at the forefront of anticipating, mitigating and responding to online harms. This work falls under our proactive and systemic change pillar. This includes our powers to regulate online services' broader systems and processes, including through the Basic Online Safety Expectations (BOSE), Social Media Minimum Age (SMMA) obligation, and industry codes and standards. It also includes our Safety by Design initiative, as well as our work anticipating and responding to emerging tech trends, opportunities and challenges.

We take a risk and harms-based approach to our work. We also recognise that combating online harm is a global challenge. We work as part of a cross-sector and multi-jurisdictional online safety ecosystem. This approach complements the role other agencies play in investigating and prosecuting crimes perpetrated online.

Statutory review of the Online Safety Act

This submission draws from and refers to eSafety's current regulatory remit under the Online Safety Act.

The [final report of the independent review of the Online Safety Act](#) was provided to the Government by the reviewer Ms Delia Rickard PSM on 31 October 2024. The Terms of Reference for the review were broad ranging and focussed on the operation and effectiveness of the Online Safety Act.

In November 2024, the Australian Government committed to legislating a Digital Duty of Care under the Online Safety Act. The duty of care will place the onus on all online

platforms to proactively keep Australians safe and prevent online harms at a systemic level.

In April 2026, the Government released its [response to the review](#). Building on the Government's existing commitment to introduce a duty of care, the Government intends to implement, wholly or partially, or further consider 64 of the 67 recommendations. As an immediate priority, the Government has committed to reforms that incentivise harm prevention.

eSafety will continue to support the Government in developing the duty of care and progressing reform arising from the Online Safety Act review.

Online hate

eSafety refers to online hate as any online communication, expression or behaviour based in hatred against a person or group based on attributes inherent to their identity, such as their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor. This is an important distinction: someone does not experience online hate because of, for example, their race, but because of the underlying form of oppression and prejudice of racism. This conceptual framing ensures the focus is on the underlying form of oppression or prejudice, rather than the aspect of identity, which should be a source of strength.

Online hate can be intersectional, meaning that a person or group can be targeted because of hateful views about multiple attributes of their identity, which can compound the severity of harm they experience.

The Online Safety Act does not include a definition of online hate. eSafety can take action where online hate material meets the threshold of our regulatory schemes, including through our complaints schemes, industry codes and standards and the BOSE. In addition, eSafety continually seeks to better understand and address online hate through its research and prevention initiatives.

Response to Terms of Reference

The nature, prevalence and impact of racism, hate and violence towards First Nations people, including trends over time

Prevalence of online hate targeted towards First Nations people

eSafety's research program supports, encourages, conducts and evaluates research about online safety for Australians.

Our [online hate research series](#) explored the prevalence, nature and impact of online hate² among adults in Australia, with a particular focus on adults from targeted groups, including First Nations adults.

Drawing on a nationally representative survey of 5,304 adults living in Australia, conducted in November 2022, we found that First Nations adults were significantly more likely to have been targeted with online hate. Over 1 in 3 First Nations adults (34%) had personally experienced online hate in the 12 months to November 2022, compared with 17% of non-Indigenous adults. In addition, 57% of First Nations adults had seen online hate in the previous 12 months, compared with 33% of non-Indigenous adults.³

eSafety's '[Keeping Kids Safe Online](#)' survey explored the benefits, opportunities and risks that the online world offers children in Australia, including First Nations children.

Drawing on a nationally representative survey of almost 3,454 children in Australia aged 10 to 17, conducted between December 2024 and February 2025, we found that 50% of First Nations children had personally experienced online hate at some point⁴; 29% had experienced this in the previous 12 months.⁵ In addition, just under 1 in 3 First Nations children (31%) had at some point someone say or post offensive or threatening things to or about them online because they were hateful of them being Aboriginal or Torres Strait Islander.⁶ Looking at all children surveyed, we found that 1 in 4 (25%) had ever seen online hate against Aboriginal and/or Torres Strait Islander people.⁷

The nature and impact of online hate targeted towards First Nations people

eSafety's [online hate research series](#) found that experiences of online hate have significant negative impacts on First Nations adults. Over half of First Nations adults surveyed who had personally experienced online hate (57%) perceived at least one negative impact following their experience, especially on their beliefs, values and identity, mental or emotional wellbeing, or their normal online behaviour or routine.

As with non-Indigenous adults, First Nations adults were most likely to have personally experienced online hate from strangers (66%) and to have been targeted on social media (66%).

² In the survey, we defined online hate as: "online communication that attacks or uses insulting or discriminatory language with reference to a person or a group on the basis of who they are – in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor."

³ eSafety Commissioner. (2025). *Fighting the tide: Encounters with online hate among targeted groups*. Australian Government. https://www.esafety.gov.au/sites/default/files/2025-02/Online-hate-report_Main-Feb25.pdf?v=1775691797629

⁴ This includes experiences where someone had said or posted offensive or threatening things to or about them because they were hateful of one or more of their identity characteristics.

⁵ eSafety Commissioner. (forthcoming).

⁶ eSafety Commissioner. (2025). *How common are personal experiences of online hate among children in Australia?* Australian Government. <https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia/snapshot-personal-experiences-of-online-hate>

⁷ eSafety Commissioner. (2025). *How common are experiences of seeing online hate among children in Australia?* Australian Government. <https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia/snapshot-seen-online-hate>

We also found that some First Nations adults may be afraid to act after seeing online hate – only 29% of First Nations adults who had seen online hate reported taking action afterwards. Among those who didn't act, First Nations adults were more likely than non-Indigenous adults to report they refrained from acting as they were afraid of what might happen as a result (19% versus 9%). In addition, just under 2 in 5 First Nations adults who had personally experienced online hate (38%) took any action following their experience.⁸

The effect of online platforms on the reach, prominence and harm caused by racism and hate directed at First Nations people

Expressions of online hate can be facilitated by a range of media and online services. There is a fluid interplay between social media, websites, messaging apps, gaming platforms, dating apps, as well as ephemeral forms of media. Social media influences, and is influenced by, a range of other media sources, including news, popular culture, marketing and advertising.

Online platforms and services make choices in the design and deployment of their services which can exacerbate harms online like racism and hate directed at First Nations people.

eSafety's [Safety by Design](#) initiative encourages technology companies to take proactive steps to embed user safety and invest in risk mitigation from the outset and throughout the product lifecycle. It is important to consider both the offline context of harms, and the holistic impact of platform design decisions and features, and how these interplay.

We have highlighted the role of recommender systems and algorithms in this section, exploring risks and impacts at a high-level which are related to platform design. eSafety is considering these and related topics as part of our [tech trends and challenges](#) program.

Recommender systems and algorithms

Recommender systems are central to how we use the internet and are integral to many online platforms and services. They select, filter and personalise content and other items across online platforms, services and applications.

When the decisions and policies shaping their design do not put users' best interests first, they can extend the reach of harmful content, such as racist or hate content, and consequently amplify its negative impact.

Recommender systems also interact with harms that already exist in society, and can draw on and exacerbate underlying social issues, such as inequality, discrimination, prejudice and oppression.

⁸ eSafety Commissioner. (2025). *Fighting the tide: Encounters with online hate among targeted groups*. Australian Government. https://www.esafety.gov.au/sites/default/files/2025-02/Online-hate-report_Main-Feb25.pdf?v=1775691797629

This applies to the online hate experienced by Aboriginal and Torres Strait Islander people, which means how recommender systems are designed, implemented and regulated is a key consideration in ensuring the safety of First Nations people online.

It is important to note that content users share and engage with online is often rooted in broader societal issues or polarising and emotionally charged debates, rather than simply a service's recommender system. A user's personal experience also impacts the potential harm of this content.

Recommender systems present unique risks and harms, which are affected by context and specific design choices and can extend beyond the impacts of individual pieces of content. There are a number of important factors, related to underlying system design, which can impact these risks and harms:

- Social media platforms overwhelmingly prioritise engagement when sorting and presenting content algorithmically, but these systems rarely distinguish between positive and negative engagement. When a user encounters content and reacts negatively, a recommender system may still treat that response as a signal to recommend more of the same content. This can facilitate increased reach and spread of harmful content.
- The impact, severity and type of harm a user may experience from recommended content varies based on a user's particular circumstances. Recommender systems rarely consider this context and may not distinguish between whether content about a sensitive topic is harmful or intended to reduce, counter or raise awareness of a harm.
- Recommending large volumes of harmful content to a user may cause cumulative effects that can be more impactful and harmful than any one individual post, creating deeper and longer lasting harm.

Given recommender systems amplify harms that already exist in online and offline settings, the impact of the whole platform design and broader social contexts must be considered from a systemic perspective.

In December 2022, eSafety published a position statement on recommender systems and algorithms, which explores the benefits and risks of recommender systems and their underlying algorithms, as well as impacts on an individual and societal level.

eSafety is currently in the process of updating this position statement, recognising that there have been a number of changes in the landscape since the paper was originally published. The updated position statement will outline current and emerging risks and harms relating to recommender systems, identify opportunities, explore regulatory challenges and provide guidance on Safety by Design measures. The updated paper considers new risks and impacts and the increasing influence of artificial intelligence (AI) in terms of both platform and service approaches and content. Publication of this paper is expected in May 2026.

Initiatives that are effective in combating racism targeted at First Nations people and reduce individual and collective harm

Industry

In addition to our complaints-based schemes for individuals, eSafety promotes proactive and systemic change within industry to enhance systems and processes and better address the risks of online harms.

Safety by Design

Our voluntary Safety by Design initiative, developed through in-depth research and consultation with industry, supports companies to consider and build in safety throughout the design, development and deployment stages of the product lifecycle.

At the heart of Safety by Design are three principles that provide platforms and services with guidance as they incorporate, assess and enhance user safety:

- Service provider responsibility
- User empowerment and autonomy
- Transparency and accountability

These foundational principles are supported by:

- **Safety by Design** foundations: educative modules that guide users through the practical steps to embed safety in their organisation's culture, policies, product features and design.
- **Two risk assessment tools** that take participants through sets of questions asking about what systems, processes and practices are in place within the businesses.
- **Industry guides** that build on the Safety by Design principles and assessment tools to further guide and support technology companies to embed safety into the culture, ethos and operations of their businesses – from the ground up.

Platforms and services are enabled to safeguard users from online hate by implementing Safety by Design measures. These include:

- Developing community guidelines, terms of service and moderation procedures that are fairly and consistently implemented.
- Putting in place infrastructure that supports internal and external triaging, clear escalation pathways and reporting on all user safety concerns, alongside readily accessible mechanisms for users to flag and report concerns and violations at the point they occur.
- Putting processes in place to detect, surface, flag and remove illegal and harmful behaviour, contact and content with the aim of preventing harms before they occur.

- Providing technical measures and tools that adequately allow users to manage their own safety, and that are set to the most secure privacy and safety levels by default.
- Establishing clear protocols and consequences for service violations that serve as meaningful deterrents and reflect the values and expectations of the users.
- Carrying out open engagement with a wide userbase, including experts and key stakeholders, on the development, interpretation and application of safety standards and their effectiveness or appropriateness.

Basic Online Safety Expectations

The Basic Online Safety Expectations (BOSE) are the Australian Government's expectations about the steps that providers of social media services, messaging, gaming and file sharing services, apps and other websites should take to keep Australians safe online.

While the BOSE are not enforceable, under the Online Safety Act, eSafety has powers to compel information from providers on their compliance with the BOSE. These powers are backed by civil penalties and form the basis for the transparency scheme under the Online Safety Act. The BOSE apply to unlawful and harmful material and activity which falls within eSafety's remit, including Class 1 and Class 2 material, cyberbullying, imaged-based abuse.

The BOSE do not specifically mention online hate; however, section 6 of the BOSE sets an expectation that providers will take reasonable steps to minimise the provision of 'unlawful and harmful' material and activity on a service. The Explanatory Statement to the BOSE states that harmful material and activity includes material and activity that should fall under a service provider's terms of use, 'as outlined in Section 14'.

Section 14 of the BOSE sets an expectation that a provider will ensure its service has terms of use, policies, and procedures in relation to the safety of end-users, as well as policies and procedures for dealing with reports and complaints. The provider is expected to take reasonable steps to ensure that penalties for breaches of its terms of use are enforced against the offending end-users (subsection 14(2)).

In relation to section 14, the Explanatory Statement to the BOSE states that "services should use their terms, policies and procedures to address material that is not necessarily unlawful or explicitly referenced in the Act, for example **hate against a person or group of people on the basis of race, ethnicity, disability, religious affiliation, caste, sexual orientation, sex, gender identity, serious disease, disability, asylum seeker/refugee status, or age**" [emphasis added]. While the Explanatory Statement does not create a specific requirement for providers to include online hate as part of their terms of use, it highlights the importance of terms of use covering that kind of material and activity.

To date, eSafety has published a number of transparency reports focused on the measures some online providers have in place to address child sexual exploitation and abuse material and activity, terrorist and violent extremist material and activity, age assurance and online hate.

Among other insights, eSafety's report on Online Hate highlighted the potential impact of major platforms not having public policy staff located in Australia, limiting their ability to take into consideration cultural and contextual information when reviewing material and applying policies. In response to questions about implementation of its hateful conduct policy in Australia, X Corp stated: "While it is ideal to make contextual assessments, it is also important to highlight that context and intent may not always be obvious to our frontline moderators or our proactive enforcement tools. We strive to get it right, but it can sometimes be hard in the absence of relevant information and context, and we're also aware of the risk of over enforcement or disproportionate enforcement if we allow subjective decision-making in the process."

Online Safety Codes & Standards

The Online Safety Codes and Standards contain mandatory systemic requirements related to unlawful material and age-restricted material across key sections of the online ecosystem, including social media, messaging, websites, generative AI, app stores and search engines. eSafety can investigate breaches of requirements under the Codes and Standards and enforce against service providers through a range of enforcement options for non-compliance, including civil penalties of up to \$49.5 million.

The Unlawful Material Codes and Standards contain measures to address the most seriously harmful online content, such as child sexual exploitation material, pro-terror material and extreme crime and violence. Pro-terror material may include ideologically motivated extremism towards First Nations people. Mandatory requirements in relation to pro-terror material focus on detecting and preventing the creation and distribution of such material; proactively removing the material as soon as practicable; providing effective user-reporting mechanisms, and appropriate and timely responses to user-reports; and notifying appropriate authorities of the material.

Social Media Minimum Age Obligation

The Social Media Minimum Age (SMMA) obligation requires providers of age-restricted social media platforms to take reasonable steps to prevent Australian children under the age of 16 from having accounts. Where eSafety considers a platform has not taken reasonable steps, eSafety has a range of enforcement options available, including civil penalties of up to \$49.5 million.

The SMMA obligation is intended to give Australian children more time to develop their digital literacy skills and resilience to navigate the risk of harms associated with social media accounts. This includes reducing the exposure of Aboriginal and Torres Strait Islander children under 16 years from online hate and other online harms occurring on age-restricted social media platforms.

eSafety is conducting its own implementation and outcomes evaluation of the SMMA obligation. The evaluation seeks to understand how the obligation is working in practice and what impacts it is having on children, young people and families. This major study will assess how the minimum age is being implemented, examine both intended and unintended impacts, and deliver strong, evidence-based insights to guide future decision making.

Prevention and Education

eSafety prioritises prevention activities that support, protect and build the capacity of those communities most at risk online. As described elsewhere in this submission, Aboriginal and Torres Strait Islander communities experience disproportionate exposure to online harms. For some communities, the use of mobile devices as a primary means of accessing the internet, high rates of device sharing and lower levels of digital literacy mean that conventional online safety advice may not be culturally appropriate or effective.

In response, eSafety undertakes ongoing actions to identify, raise awareness and address online harms affecting First Nations communities. These actions are grounded in research and informed by meaningful engagement and co-design with First Nations organisations and communities. This ensures resources are culturally safe, responsive to emerging issues and reflect the real-world experiences of the communities we support.

A dedicated [First Nations](#) section of the eSafety website, featuring culturally appropriate guidance, imagery and support tools was launched in March 2023. Within the dedicated section we maintain a webpage specifically focused on online hate and abuse, featuring fit-for-purpose guidance on strategies to deal with online abuse, preventing further contact from those perpetrating abuse, and reporting mechanisms available. This webpage embeds videos we have developed in collaboration with First Nations organisations and creatives, allowing us to communicate online safety concepts in a way that is accessible and engaging. The videos feature culturally tailored animations as well as filmed case studies of First Nations people share experiences of online harassment. Some of our videos and audio recordings have been translated into 17 Aboriginal and Torres Strait Islander languages, increasing the accessibility of this information, especially for remote communities.

eSafety research has indicated there is an ongoing need for online safety information among Aboriginal and Torres Strait Islander parents and caregivers and their children. The same report found that Aboriginal and Torres Strait Islander children are almost three times more likely to have experienced online hate speech than the national average.⁹ In July 2025, eSafety released two online safety guides designed for two-way learning between parents and carers and First Nations children and young people. These guides, *Safer Together!* and *Leaving Deadly Digital Footprints!*, were co-designed with First Nations children, parents, and carers, and use storytelling, case studies and interactive activities to learn safe and positive online behaviours. The guides feature content on hate, racism, violence and provide First Nations young people and their families with practical skills and encourage help seeking behaviours.

Through the Online Safety Grants Program, eSafety supported First Nations organisations to deliver tailored workshops and online safety education to remote First Nations communities. Our Preventing Tech-based Abuse of Women Grants Program provides a total of \$10 million in grant funding from 2023 to 2028 across a range of

⁹ eSafety Commissioner (2022). Cool, beautiful, strange and scary: The online experiences of Aboriginal and Torres Strait Islander children and their parents and caregivers. https://www.esafety.gov.au/sites/default/files/2023-03/Cool_beautiful_strange_and_scary_report.pdf?v=1776821929793

initiatives aiming to improve the safety of Australian women and their children through the prevention of technology-facilitated gender-based violence. This may include projects that target people who perpetrate technology-facilitated abuse and/or changing attitudes and behaviours in the broader community, as well as projects that specifically target women and children. Within Round 2 and Round 3 specifically, up to \$600,000 per round was available to organisations with a commitment to delivering projects with and for communities that focus on the prevention of tech-based abuse of First Nations women.

eSafety utilises its communication channels to reach First Nations audiences with relevant information, including through a dedicated mailing list, social media, and distribution of physical resources. We also exhibit and present at conferences and events focused on First Nations policy, governance, and sector-specific issues.

The threat posed by ideologically motivated extremism towards First Nations people and the role of intelligence and law enforcement agencies in protecting the community from that threat

Online extremism can take different forms and may impact communities in different ways. For example, it may take the form of online hate or abuse, with members of at-risk groups being more likely to encounter online hate or be targeted with online abuse from those who hold extremist views.

While eSafety does not have a specific focus on extremism, the issue of online extremism can intersect with eSafety's activities where it involves illegal and restricted content covered by eSafety's Online Content Scheme. When considering illegal and restricted online content, eSafety must decide whether it would be defined as Class 1 or Class 2 material under the National Classification Scheme. Class 1 material is material that would be refused classification under the National Classification Scheme, including material that advocates terrorist acts, or that promotes, incites, or instructs in matters of crime or violence. Class 2 material includes material that would be classified R 18+ or X 18+ under the National Classification Scheme. Under the Online Safety Act, eSafety can consider a range of informal and formal compliance options when seeking to remove or limit access to illegal and restricted online content.

The vast majority of reports to eSafety relate to child sexual exploitation and abuse material (85% in 2024-25). Less than 2% of reports in the same period relate to content that advocates terrorist acts or material that incites or instructs in matters of crime or violence.

eSafety has specific powers and obligations regarding the sharing of information with law enforcement agencies. eSafety may disclose information to law enforcement agencies and other regulatory bodies if it is satisfied that the information will assist them to perform their functions or powers.¹⁰ eSafety must notify a member of an Australian police force if material is considered to be of a sufficiently serious nature.¹¹

¹⁰ Online Safety Act 2021 (Cth), s 212.

¹¹ Online Safety Act 2021 (Cth), s 224.

Some eSafety resources are relevant to understanding and preventing online harms which may be related to extremism. eSafety also has a range of resources to help people develop the critical skills they need to navigate the online world more safely. eSafety has also developed resources for parents and carers, educators, and young people on dealing with [distressing and violent content](#).

The effectiveness of avenues for reporting and responding to racism against Aboriginal and Torres Strait Islander people, including the consistency, timeliness and appropriateness of outcomes across jurisdictions and institutions

Complaints-based regulatory schemes

eSafety administers four complaint schemes under the Online Safety Act, addressing the following online harms: cyberbullying of children; cyber abuse of adults; non-consensual sharing of intimate images; and, illegal and restricted content.

Where the online material reported to us meets the legislated thresholds, eSafety can issue removal notices to the online service on which the content is posted and the hosting service that hosts the content on the service. Where the online service does not comply with a removal notice, eSafety can take enforcement action. These schemes are ‘technology-neutral’ meaning they cover AI-generated images, text, audio and other content. For adult cyber abuse, cyberbullying and image-based abuse, eSafety can also issue notices to the end-user responsible for posting the material.

Across the four schemes, investigators review a high volume of material. eSafety prioritises complaints that require the quickest compliance and enforcement action. Some reports are detailed and may require a longer time to assess, while others are more straightforward. When material reported is of the highest priority, the reporter can expect a response from eSafety within two business days.

Adult Cyber Abuse Scheme

The adult cyber abuse scheme covers online material that an ordinary reasonable person would conclude was likely intended to have the effect of causing serious harm to a particular Australian adult, and which an ordinary reasonable person in the position of the Australian adult would regard as being menacing, harassing or offensive in the circumstances.

The adult cyber abuse scheme is a safety net to be used when a complaint has been made to an online service provider, but the online service provider has not removed the material. The material must be provided on a social media service, relevant electronic service or designated internet service and can include posts, comments, memes, images or videos.

eSafety cannot take formal action against content targeting a group or organisation. For eSafety to be able to act on a complaint, the material must target a particular Australian adult.

The scheme is not limited to any specific personal attribute, including abuse relating to an individual's race and religious beliefs and activities. However, hateful elements within a post (for example, the use of ethnic slurs) may be considered as a relevant factor in determining whether the content meets the threshold of adult cyber abuse.

The adult cyber abuse scheme enables eSafety to give formal notices to the service, end-user or hosting service provider to remove the content if it breaches the Online Safety Act. In some cases, we may refer a complaint to the online service for consideration if we believe the content is likely to violate that service's terms of service.

Cyberbullying Scheme

eSafety's cyberbullying scheme covers online material that an ordinary reasonable person would conclude was likely intended to have the effect of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating a particular Australian child or young person (under 18).

Like the adult cyber abuse scheme, the cyberbullying scheme is a safety net for when a complaint has been made to an online service provider, but the service has not removed the material. The cyberbullying scheme captures a broader set of online harms which can include online hate or vilification but is not limited to abuse referencing a specific set of personal attributes. It is restricted to behaviour directed towards an individual and does not capture cyberbullying directed towards a group of people.

The cyberbullying scheme also enables eSafety to give end-user notices requiring the end-user to refrain from posting any further cyberbullying material and/or apologise to the child who was the target, in addition to removing the cyberbullying material.

Complaints received from persons identifying as Aboriginal and Torres Strait Islander

Since the Online Safety Act came into effect on 23 January 2022, eSafety has received more than 1,500 complaints under the Adult Cyber Abuse and Cyberbullying schemes from persons identifying as Aboriginal and Torres Strait Islander.

These complaints include reports of threats of violence, incitement of self-harm and suicide, as well as hate speech and content on hate pages. Most complaints were submitted for harm affecting persons under the age of 18, with the next highest reporting cohort comprising adults aged 25–39 years.

Among complaints involving persons under 18 years of age, females account for more than three times the number of reports made by males for hate and violence related harms, indicating a gender disparity in reporting of these harm types to eSafety within this age group.

Conclusion

eSafety is pleased to have the opportunity to provide context and evidence on racism, hate and violence directed at Aboriginal and Torres Strait Islander peoples, from its vantage point as Australia's online safety regulator. We will continue to draw on the levers available to us to support First Nations communities to have safer, more positive experiences online. We welcome the opportunity to provide additional evidence or clarify any aspects of the submission should it assist the Committee's inquiry.