

ONLINE SAFETY – OVERARCHING

Topic	Page number
Government's online safety agenda	2
BOSE, industry codes and OSA review	4
Women's safety	7
Non-compliance of X (Twitter) under the BOSE	9
Deepfake intimate images and AI-enabled online abuse	11
Online hate speech	13
Preventing smartphone use until age 14 ('Wait for 8')	16
Sexual Extortion	18
Industry standards and encryption	21
Eating disorders	23
Background	30

Cleared by: s22(1)(a)(ii)

Division: DIV - Online Safety Media and Platforms

Created: 11 January 2024

Last Updated 7 May 2024

QUESTION: What is this Government doing about online safety?

Australia has a strong track record in online safety and a world-leading online safety regulator in the eSafety Commissioner.

Keeping Australians safe online is, and will always be, a top priority for the Albanese Government.

Implementing the Online Safety Act remains a priority for the Government, which is why eSafety's ongoing base funding was quadrupled in the 2023-24 Budget – making sure the regulator has the resources it needs.

But the online world is continually changing and Australia's approach needs to evolve. This is why we are tackling gaps in the current regulatory framework.

While the Online Safety Act has a wide scope, we know there are issues with the broader online ecosystem which can have safety implications for Australians.

We have brought forward the independent review of the Online Safety Act, which will be completed this year. The review will make sure our laws and regulations are fit for purpose and also keeping pace with emerging online threats and harms.

We are progressing a range of work streams to address these gaps, including work to improve online dating safety, addressing mis and disinformation, conducting a trial of age assurance technologies, and commencing a review of classification reforms with the states and territories.

The Albanese Government is also making sure there is cross-Government coordination on the regulation of online harms. To achieve this, I convene a bi-annual meeting of Federal Ministers with responsibility for addressing online harms so we can improve online safety for all Australians, across all the vectors through which harm occurs.

QUESTION: How are industry codes and BOSE improving online safety? What will the Online Safety Act review consider?

The Online Safety Act provides the eSafety Commissioner with important powers to compel transparency from the digital industry, with respect to how they are meeting the Government's Basic Online Safety Expectations.

The eSafety Commissioner's October 2023 transparency report indicates that detection tools and technologies are not being used consistently by industry to address child sexual exploitation and abuse material, and that more can be done.

All child sexual exploitation and abuse material is horrific and I expect industry to be doing more to rid the internet of this abhorrent material.

The Government welcomes the eSafety Commissioner's most recent decision to issue reporting notices to six major companies regarding terrorist and violent extremist material and activity on their platforms. These companies will be required to answer detailed questions on steps they are taking to protect Australians from such material on their platforms.

We are concerned that the eSafety Commissioner continues to receive reports of terrorist and violent extremist material being shared and reshared on platforms and messaging services, including of the 2019 terrorist attack in Christchurch.

Industry has a responsibility to prevent the spread of this material and to prevent online radicalization on their platforms. The Government expects industry to take this responsibility seriously and to cooperate with the eSafety Commissioner through the exercise of her powers.

These transparency powers work hand-in-hand with another core element of the Online Safety Act, mandatory, enforceable Industry Codes.

The eSafety Commissioner has registered six industry codes and is developing binding industry standards. These measures outline steps the online industry must take to address seriously harmful material, including child sexual exploitation and terrorist material.

The Expectations and the industry codes are core elements of our online safety framework, but with the online world changing quickly, we need to make sure our laws remain fit-for-purpose.

I recently announced the appointment of Ms Delia Rickard PSM to undertake the independent review of the Online Safety Act. The Review is a broad-ranging examination of the operation and effectiveness of the Act.

This includes looking at eSafety's powers in relation to the industry codes and the Expectations, the penalty and enforcement regime, and gaps in the legislation.

Public consultation for the Review will commence in the first half of 2024, with a final report to be provided to Government later this year.

Work to keep our online world safe is ongoing – every day new challenges emerge. Our Government will continue to hold industry to account and put the safety of Australians first.

QUESTION: What is this Government doing to protect women from being stalked, tracked and abused online?

Keeping Australians safe is a top priority for the Albanese Government. And we know that when it comes to comes to online abuse and harassment, Australian women are disproportionately affected. Sadly, seventy per cent of reports of online harm received by the eSafety Commissioner are from Australian women and girls.¹

We also know that technology-facilitated abuse has become a key part of domestic, family and sexual violence, with one in three Australian adults having experienced technology-facilitated abuse from a current or former partner.² That is why the Government provided the eSafety Commissioner with \$16.6 million to develop a new support service to provide support to victim-survivors of technology facilitated abuse, and the frontline workers assisting them.

We are also funding an advertising campaign to raise awareness across Australia about the new protections available for women who have

¹ <https://www.esafety.gov.au/key-issues/domestic-family-violence>

² ANROWS (2022). Technology-facilitated abuse: National survey of Australian adults' experiences. Retrieved from www.anrows.org.au/publication/technology-facilitated-abuse-national-survey-of-australian-adults-experiences/

experienced serious online abuse. And we are providing grant opportunities for local, community-based organisations for online safety initiatives that assist and protect women and children from technology-facilitated abuse.

The Government is also acting to protect women using online dating services, who all too frequently receive harassing or abusive messages, or experience in-person violence. I have asked the online dating industry to do more to protect Australians through a new industry code. The online dating industry has until the middle of the year to have the code in place. If it is not strong enough – or the code fails to improve protections for Australians – I will not hesitate to take further action.

The Government is determined that women should be free to use the internet safely. We will not allow the voices of women and girls to be silenced, or to be pushed out of the online environment. I have recently announced an independent review of the Online Safety Act which will be completed within the current term of Government. This review will make sure that the eSafety Commissioner has all the tools needed to keep women safe online.

QUESTION: Is the Government concerned about X Corp's non-compliance with Australia's Online Safety Act? ?

The eSafety Commissioner has issued X Corp with two reporting notices under the Basic Online Safety Expectations framework.

The first reporting notice was sent to a range of digital platforms in February 2023, including X Corp, and required information about how they are tackling child sexual exploitation and abuse. X Corp failed to meet its reporting obligations and as a result, the Commissioner issued X Corp an infringement notice for \$610,500 for its non-compliance. X Corp did not pay the infringement notice and in November 2023 it sought judicial review in relation to this matter.

Separately, in December 2023, the Commissioner initiated civil penalty proceedings against X Corp in the Federal Court for failure to comply with the reporting notice.

As both the judicial review and civil penalty matters are currently before the Court, it would not be appropriate to comment on these proceedings.

The second reporting notice was issued to X Corp in June 2023 asking for information on the steps it is taking to address online hate speech on its platform. eSafety found that X Corp has significantly reduced its content moderation and trust and safety staff since the platform was acquired in

October 2022, and that the average time taken to respond to user reports of hateful conduct has increased.

These findings raise significant concerns about X Corp's capacity to address online hate on its platform, and that not enough is being done to tackle child sexual abuse material.

X Corp must do more to improve user safety on its platform. The Government's expectations are clear and we will continue to monitor how industry is meeting its responsibilities and compliance with the Online Safety Act.

The Albanese Government has brought forward the independent review of the Online Safety Act 2021 to make sure the eSafety Commissioner has the right powers to hold industry to account, including whether the existing penalty regime works as an effective deterrent to industry non-compliance.

In the 2024-25 Budget, the Government provided eSafety with an additional \$1.4 million over two years to boost eSafety's internal legal and compliance functions. This builds on last year's budget which saw a quadrupling of eSafety's ongoing base funding.

QUESTION: What is the Government doing to address deepfake intimate images and AI-enabled online abuse?

Every Australian deserves to live free from violence and abuse, and this includes being free from image-based abuse and harassment. We've seen recent examples of high profile women being targeted by abuse with material created using generative AI, but you don't need to be a celebrity for this to happen. All Australians should know that if intimate images are shared of them, no matter how they were created, they have opportunities for redress.

Deepfakes are fake images, videos, or sound files which depict people doing or saying things they did not actually do or say. Regardless of how the content is generated it can have serious impacts on victims' lives.

Australia's Online Safety Act is 'technology neutral'. This means that eSafety's complaints-based investigations schemes can capture these deepfake AI-generated images, text, audio and other content.

Image-based abuse, cyberbullying material and adult cyber abuse can all be reported to eSafety, regardless of how the content was generated. The eSafety Commissioner has powers to have this harmful content removed and, depending on the circumstances, can issue removal notices to services or individuals and issue fines for non-compliance.

eSafety can also refer matters to law enforcement if appropriate. The Criminal Code makes it an offence to use a carriage service to menace, harass or cause offence. The Attorney-General will introduce legislation to ban the creation and non-consensual distribution of deepfake pornography. This will make creating and sharing sexually explicit material without consent against the law and subject to serious criminal penalties.

I strongly encourage anyone who is depicted in an intimate image or video posted online without their consent, or has been the subject of cyberbullying or adult cyber abuse, to go to esafety.gov.au for more information on the support that eSafety can provide.

QUESTION: What is the Government doing to address online hate speech and doxxing?

There is no place for racism or hatred in Australia – offline or online.

The Australian Government believes that all people are entitled to respect, equality, dignity, and to be free from hatred or harassment. We will continue to oppose extremism, hatred, ethnic division and incitement to violence in all its forms.

The eSafety Commissioner has powers under the Online Safety Act to address online material targeted at an Australian adult that is menacing, harassing or offensive, and intended to cause serious harm – which includes doxxing material and hate speech where it meets this threshold. The eSafety Commissioner can also act where online material incites violence or promotes crime or terrorism.

The Albanese Government has committed to stronger privacy protections for Australians in our response late last year to the landmark review of the Privacy Act, and the Government will be bringing forward legislation that will include measures to protect Australians from the malicious use of their personal and private information (known as doxxing).

Important work to strengthen laws against hate speech is being led by the Attorney-General, the Hon Mark Dreyfus KC MP.

The Government has also asked for the Review of the *Online Safety Act 2021* to consider what more can be done to address hate speech directed at groups or communities online, with the Review to be completed in this term of government.

The eSafety Commissioner is improving industry transparency on online hate speech through the Government's Basic Online Safety Expectations framework. In January 2024, the Commissioner published a transparency report on how Twitter (now X Corp) is addressing online hate on the platform. The Commissioner found that X Corp has significantly reduced its content moderation and trust and safety staff since the platform was acquired in October 2022, and that the average time taken to respond to user reports of hateful conduct has increased.

At the same time, the Government has proposed a number of amendments to strengthen the Basic Online Safety Expectations Determination to increase industry accountability for protecting Australians online. The proposed changes include encouraging services to detect and address online hate speech

that breaches a service's terms of use. Public consultation on the proposed amendments closed on 16 February 2024.

I want to reiterate that hate speech has no place in Australia – offline or online. The Government and our online safety regulator take this issue very seriously and we are watching closely to make sure platforms play their part in preventing this material circulating online.

QUESTION: Do you agree with calls for parents to keep their children off smartphones until age 14 (the 'Wait for [Year] 8 campaign)?

In the digital age, every family has to make decisions about how to manage their children's social media use, and how to support their children to get the most out of the internet – in a safe and healthy way.

That is why the Australian Government is committed to empowering parents and carers with the information they need to navigate these decisions. The eSafety Commissioner makes available a wealth of resources and advice on managing screentime, and taking care of mental health while using social media.

We are also upskilling Australian kids to deal with digital literacy challenges. The Government is providing \$6 million over three years to the Alannah and Madeline Foundation to deliver its digital and media literacy education products free in Australian schools. This funding will also support the development of new modules for the eSmart Digital Licence+ for primary

students aged 5 to 9 years of age, to support the increasing number of young children who are active online.

But the responsibility for staying safe online cannot and should not fall solely parents and children themselves. It is critical that industry lift its game when it comes to addressing harms that can come to users, especially children and young people.

That is why, in November 2023, I commenced public consultation on amendments to the Online Safety (Basic Online Safety Expectations) Determination 2022 which currently applies to a range of online platforms, including social media services. The determination outlines the Government's expectations on platforms in how they are keeping users safe, and the amendments proposed would establish new expectations, including that services consider the best interests of children in the design and operation of their services.

Public consultation on the BOSE reforms closed in February and my department is currently considering feedback from the process.

I have also commenced an independent review of Australia's Online Safety laws, to examine their operation and effectiveness and to ensure they can address new and emerging harms impacting all Australians online, including children. The review is being led by Ms Delia Rickard PSM, and public consultation is underway with a report due to Government by 31 October 2024.

The review of the Online Safety Act is an important opportunity to consider what further powers the regulator might need to address harms in the online environment. I encourage all those who with an interest in online safety to to engage through the public consultation process, so we can ensure our online safety laws remain strong, and responsive to new and emerging harms.

Sexual extortion (sextortion)

Threatening to share intimate pictures online without consent, for money or for other reasons, is a crime. Possessing or sharing such material when it involves young people under the age of 18 is a very serious crime and constitutes child sexual abuse.

It's important that Australians, particularly young people who are often the target of sexual extortion, know what to look for, and where to go for help. We need people to know this is not something to be ashamed of, and that they can speak with their friends, a trusted adult, or go to eSafety if they are targeted.

I am advised that sexual extortion reports account for the majority of image-based abuse reports to eSafety, with reports predominantly from young men.

The eSafety Commissioner's website has valuable guidance on how to deal with sexual extortion. eSafety can also refer victims to counselling and support services, and to law enforcement if appropriate.

The Online Safety Act's image-based abuse scheme means that the eSafety Commissioner can issue a removal notice to perpetrators and the platforms that host the material. They must remove those images from the internet within 24 hours. If they do not comply they face a penalty of up to \$782,500.

Important work is also being done by the Australian Federal Police. Working together with the Australian Transaction Reports and Analysis Centre (or AUSTRAC as it is more commonly known), the AFP shut down more than 1,000 Australian bank, financial services and digital currency accounts linked to offshore organised syndicates sexually exploiting Australian teenagers between June and December 2022.

The eSafety Commissioner also issued a set of reporting notices under the Basic Online Safety Expectations to platforms including Twitter (now X), TikTok and Google, requiring reports on a range of issues such as sexual extortion.

The information received through these reports has shown that digital platforms need to be doing more to prevent children being sexually extorted on their services.

The review of the Online Safety Act is an important opportunity to consider what further powers the regulator might need to address this serious challenge. I encourage all those who are concerned to engage through the public consultation process, which is underway and closes on 21 June 2024.

QUESTION: Will the Government step in to prevent eSafety's industry standards breaking encryption?

The industry codes and standards process, one of the important tools established under the Online Safety Act 2021, is key to preventing and restricting access to illegal and harmful material. The registered industry codes and eSafety's draft industry standards are focused on the most seriously harmful online content, including child sexual exploitation material and pro-terror material.

The development and adoption of standards are a matter for the eSafety Commissioner, as the independent regulator. I understand that eSafety is closely considering feedback from public submissions on their draft industry standards for Designated Internet Services (DIS) and Relevant Electronic Services (RES).

The Albanese Government believes that industry is primarily responsible for the harms that occur on its platforms. This means that industry must take stronger measures to address the hosting and sharing of child sexual

exploitation material and pro-terror material on their services – that is what these codes and standards seek to achieve.

Having said that, the Government's clear position remains that nothing in the Online Safety Act requires service providers to build systemic weaknesses into their encrypted services or render methods of encryption less effective.

eSafety have also been clear in this regard with public statements confirming that any obligations under the standards will not require industry to break or weaken end-to-end encryption, monitor the text of private communication or indiscriminately scan large amounts of personal data.

I welcome industry's close engagement with eSafety in the development of industry codes and standards. It is important that the draft standards strike the right balance between protecting the online safety of Australians, and what is technically feasible and proportionate for industry.

QUESTION: What is the Government doing to address eating disorder material on social media?

Eating disorders are among the most complex and harmful mental illnesses, and recovery can be long and extremely difficult. The Albanese Government takes this issue extremely seriously.

Eating disorders can have many contributing factors, which can include material on social media. The findings from Reset Australia in relation to the way pro-eating disorder material is recommended on young people's social media feeds, and the failure of content moderation to remove harmful material, is deeply concerning. The Government is committed to addressing harms in the online environment, particularly those affecting young people.

That is why, in November 2023, I commenced public consultation on amendments to the Online Safety (Basic Online Safety Expectations) Determination 2022 which currently applies to a range of online platforms, including social media services. The determination outlines the Government's expectations on platforms in how they are keeping users safe, and the amendments proposed are designed to address emerging harms.

This includes new additional expectations that services: promote user safety in the design and operation of their recommender systems; that services consider the best interests of children; and take reasonable steps to detect breaches of their terms of use.

Public consultation on the BOSE reforms closed in February and my department is currently considering feedback from the process.

I have also announced an independent review of Australia's Online Safety laws, to examine their operation and effectiveness and to ensure they can address new and emerging harms impacting all Australians online, including children.

Delia Rickard PSM is leading the review, with its Terms of Reference announced in February 2024. The Government is looking forward to the findings from the review, expected later this year, and will act accordingly to ensure our Online Safety Act remains world-leading.

Also in this area, the Government has funded the eSafety Commissioner to award grant funding to reduce the impacts of online harms, with the Butterfly Foundation – the national charity for Australians impacted by eating disorders and body image issues - receiving nearly \$277,000 under the Program.

The eSafety Commissioner's website has information and resources to help Australians to stay safer and have more positive experiences online, including dedicated resources for parents and young people - at www.esafety.gov.au.

Addressing eating disorders is a complex policy task and the Government welcomes input from a diverse range of voices on this issue. Government, parents and carers, the mental health sector and digital platforms all have a role to play in making headway against this complex and dangerous illness.

Background

s47C



Contact: Andrew Irwin (Online Safety Branch) §22(1)(a)(ii)