



Australian Government

**Department of Infrastructure, Transport,
Regional Development and Communications**

Submission

House Select Committee on Social Media and Online Safety

January 2022

Introduction

The Department of Infrastructure, Transport, Regional Development and Communications (the Department) welcomes the opportunity to make a submission to the House Select Committee's inquiry into social media and online safety.

The Department is responsible for providing online safety policy advice to the Government. We work closely with the eSafety Commissioner, Australia's online safety regulator, to deliver the Government's online safety objectives.

This submission provides:

- Information about the range of online harms faced by Australians on social media and other online platforms.
- The Australian Government's policy approach to keeping Australians safe online.
- An overview of the Australian Government's transparency and accountability requirements of social media platforms and online technology companies regarding online harms.

Key points

- The online industry has the primary responsibility to create safe online spaces for their users. As private businesses, online service providers are responsible for user safety, and are accountable for their users complying with the terms of service. The Australian Government plays an important role in holding industry to account and providing a 'safety net' for when platforms fail to protect Australians.
- No single regulatory framework can address the broad scope of online harms. There is complementary work across Government to address various online harms, including the *Online Safety Act 2021* (the Act) and subordinate legislation, the Australian Code of Practice on Disinformation and Misinformation, and the proposed privacy and defamation reforms.
- The Act comes into effect on 23 January 2022 and introduces new and strengthened schemes to keep Australians safe online.

Online harms experienced by Australians

The internet has provided great social, educational and economic benefits. However, there are also risks when engaging online and a broad range of harms can occur. These harms include:

- Cyberbullying and cyber abuse.
- Non-consensual sharing of intimate images.
- Abhorrent violent material.
- Child sexual abuse material.
- Exposure to harmful material, including suicide and self-harm content and dangerous viral challenges.
- Online hate speech and racism.
- Trolling and volumetric attacks.
- Harmful online advertising.
- Misinformation & disinformation.
- Misuse/breach of personal information by digital platforms.
- Online defamation.
- Use of a carriage service to menace, harass or cause offence.
- Terrorist and violent extremist exploitation of the internet.
- Online scams.

Many of these harms also occur offline, however social media and other online services provide a vector to distribute content quickly, which can exacerbate the nature of harm or increase its impact. Unfortunately, it is impossible to prevent all harm that occurs online, just as it is impossible to prevent all harm offline.

The table at [Attachment A](#) sets out how Australia's regulatory framework addresses these online harms, including the department responsible for leading the work and those with an interest.

Australian Government's policy approach to online safety

This submission focuses on matters within the Department's policy responsibilities. To provide context we briefly cover some of the other work occurring across Government, however, we defer to the responsible departments and agencies on the detail of the work underway in their portfolios.

Current online safety framework

Australia's current online safety regulatory framework (as at 12 January 2022) includes the *Enhancing Online Safety Act 2015* (EOSA) and Schedules 5 and 7 of the *Broadcasting Services Act 1992* (BSA). Schedules 5 and 7 of the BSA (added in 1999 and 2007, respectively) form the current online content scheme and interact with the EOSA. The EOSA came into effect in 2015 as a framework to protect Australian children online and established the eSafety Commissioner (initially the Children's eSafety Commissioner). The EOSA was amended in 2017 to expand the Commissioner's remit to include all Australians, and in 2018 to introduce the image-based abuse scheme. The current framework will shortly be repealed and replaced by the Act.

Following the 2019 Christchurch terrorist attacks, the eSafety Commissioner was also provided with a power under the *Criminal Code 1995* to issue a notice formally advising a content service or hosting service provider that its service is providing access to or hosting abhorrent violent material. eSafety's notice powers do not require the abhorrent violent material to be removed. However, if a service provider is later prosecuted for failing to remove or cease hosting abhorrent violent material, the notice can be used in legal proceedings to show recklessness regarding the abhorrent violent material.

Online Safety Act 2021 (the Act)

The Australian Parliament passed the Act on 23 June 2021 and it comes into effect on 23 January 2022. The Act replaces the current online safety framework contained in the EOSA and Schedules 5 and 7 of the BSA. The Government's policy intent that the rules and protections Australians enjoy offline should also apply online informs this legislation, and the Act provides a safety net for people when things go wrong online.

Basic Online Safety Expectations (BOSE)

In recognition of the primary role of industry to keep their users safe, the BOSE places greater responsibility on service providers to provide safer services for Australian users. The Act sets out the core requirements for the determination of the BOSE for social media services, relevant electronic services and designated internet services and the requirements for compliance reporting by industry.¹ Failure to provide reports to the eSafety Commissioner on request can lead to civil penalties.

The BOSE will be set out in an instrument made by the Minister, and includes:

- core expectations already set out in the Online Safety Act;
- a number of additional expectations to improve protections for users; and
- reasonable steps to provide guidance to industry on how to show they are meeting the BOSE.

The BOSE articulates the Government's minimum safety expectations of online service providers, establishing a benchmark for online service providers to take proactive steps to protect the community from abusive conduct and harmful content online. The BOSE will be made prior to the commencement of the Act.

Public consultation on a draft BOSE determination occurred from 8 August 2021 to 12 November 2021. 77 unique submissions were received from a range of private citizens, civil society groups, commercial organisations and industry bodies as well as 1072 emails expressing concern about the impacts of internet pornography. The Minister will take these views into account in finalising the BOSE.

Cyberbullying scheme

Cyberbullying material includes online communication to, or about a specific Australian child that is intended to have an effect and likely to have the effect of seriously threatening, intimidating, harassing or humiliating the child. It must be communicated through a social media service, relevant electronic service or designated internet service (as defined in the Act). It can include posts, comments, emails, messages, memes, images and videos.

¹ See the section below on transparency and accountability requirements for further information on BOSE reporting requirements.

The cyberbullying scheme in the Act continues the existing cyberbullying scheme set out in the EOSA, which provides a complaints based take-down scheme for cyberbullying material affecting Australian children, for social media services. It builds on this scheme by reducing the take-down time for material from 48 hours to 24 hours and extending the reach of the scheme to all types of online services used by Australian children including websites, apps and online games.

The scheme includes the following elements:

- A complaints scheme where a person may make a complaint about cyberbullying material that targets an Australian child. Generally, the complainant must have first reported the material to the relevant online service provider before asking eSafety to issue a notice to the provider requiring removal of the cyberbullying material.
- Investigative and information gathering powers for eSafety to assess complaints about cyberbullying material targeting an Australian child and decide what action is available.
- Removal powers, which allow eSafety to issue notices to online service providers, hosting service providers and to end-users who have posted cyberbullying material, requiring them to remove the material. Notices to end-users can also require that the person stop posting cyberbullying material directed to the targeted child and apologise to them.
- Enforcement actions available to eSafety where there has been a failure to comply with notices. This includes taking injunctive action against end-users and seeking civil penalties for online service providers who fail to remove material in response to a notice.

Adult cyber abuse scheme

Cyber abuse material includes online communication to, or about a particular Australian adult, which is menacing, harassing or offensive and is intended to cause them serious harm. It must be communicated through a social media service, relevant electronic service or designated internet service. It can include posts, comments, emails, messages, memes, images and videos.

The adult cyber abuse scheme is intended as 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. It includes the following elements:

- A complaints mechanism where a person may make a complaint about adult cyber abuse material that targets an Australian who is 18 years or older.
- Investigative and information gathering powers for eSafety to assess complaints of adult cyber abuse and decide what action is available.
- Removal powers, which allow eSafety to issue notices to online service providers, hosting service providers and to end-users who have posted adult cyber abuse material, requiring them to remove the material within 24 hours. eSafety's removal powers only come into effect if a complaint has first been made directly to an online service provider and they have failed to remove the material.
- Enforcement options, which are available to eSafety where there has been a failure to comply with a notice. These range from issuing a formal warning to seeking civil penalties.

Under the Act, 'adult cyber abuse' is reserved for the most severely abusive material intended to cause serious physical or psychological harm, including material which sets out realistic threats, places people in real danger, is excessively malicious or is unrelenting. In determining whether material is adult cyber abuse material, the material must be intended to cause serious harm (physical or psychological) **and** be menacing, harassing or offensive in all the circumstances. This test in section 7 is intentionally high because adults are expected to be more resilient than children, and is intended to provide balance between protection from harm and freedom of expression.

Image-based abuse scheme

Image-based abuse is sharing online, or threatening to share, an intimate image without the consent of the person depicted. The image or video itself may have been initially obtained with the consent of the victim (for example, they may have agreed to the image or video being taken or may have sent it to the end-user), or it may have been accessed without their consent (for example, through hacking or through it being shared with an end-user by another person).

The Act continues the existing complaints based take-down scheme, but allows the eSafety Commissioner to more rapidly remove material by reducing the time within which platforms or end-users must take down this content from 48 hours to 24 hours. The scheme includes:

- The general prohibition on image-based abuse allows eSafety to take action against a person (end-user) who shares online, or threatens to share, an intimate image without the consent of the person shown. An 'intimate image' can include a video.

- A complaints system where a person may make a complaint about breaches of the general prohibition on image-based abuse.
- A system under which a person may object to an intimate image remaining online even if the person depicted originally consented to the intimate image being shared.
- Investigative and information gathering powers for eSafety to assess complaints about image-based abuse and decide what action is available.
- Removal powers which allow eSafety to issue notices to online service providers and end-users requiring them to remove intimate images which are the subject of a valid complaint or objection.
- Remedial direction powers, which allow eSafety to require an end-user, who has breached the general prohibition on image-based abuse, to take actions specified by eSafety to reduce the risk of further breaches (such as deleting images from their devices).
- Enforcement actions available to eSafety where there has been a breach of the general prohibition or a failure to comply with a notice or direction. These options range from formal warnings to seeking civil penalties.
- If an end-user has been subject to three or more civil penalties for image-based abuse, this fact can be a circumstance of special aggravation in any criminal prosecution for an offence under s474.17A of the *Criminal Code Act 1995*. Criminal prosecutions are a matter for the relevant police force.

Online content scheme

The online content scheme regulates illegal and restricted online content that ranges from the most seriously harmful material (such as videos showing the sexual abuse of children or advocating terrorism), through to content which is inappropriate for children (such as online pornography). This content is defined as class 1 (seriously harmful content that has been or would likely be refused classification) and class 2 material (content that has been, or would likely be, classified as either X18+ or Category 2 restricted, or R18+ or Category 1 restricted, because it is considered inappropriate for general public access and/or for children and young people under 18 years old).

The Act strengthens the existing online content scheme contained in Schedules 5 and 7 of the BSA, including by empowering the eSafety Commissioner to seek the removal of class 1 online content, no matter where it is hosted in the world.

The scheme includes:

- A complaints scheme where a person can make a complaint about:
 - online material that they believe to be illegal or should be restricted
 - breaches of service provider rules and civil penalty provisions under the online content scheme, and
 - breaches of industry codes or standards.
- Investigation and information gathering powers for eSafety to assess complaints, or investigate certain matters on its own initiative, and decide what action to take.
- Removal and restriction powers which allow eSafety to, in certain circumstances, issue notices that direct online service providers to remove material (or remove access to material) from their services or ensure that access to certain types of material is restricted.
- Powers to register industry codes and/or industry standards that will regulate illegal and restricted online content.
- Powers to determine service provider rules for certain online service providers.
- Enforcement actions, which are available to eSafety where there has been a failure to comply with a notice or other powers under the online content scheme. These include seeking civil penalties for online service providers who fail to remove material in response to a notice.
- Powers to seek a Federal Court order, which seeks to stop the provision of certain online services where the continued operation of the service represents a significant community safety risk.

Industry codes and standards

The Act requires the registration of strengthened industry codes that will require the Australian online industry to do more to support Australian households to manage their access to harmful online content under the online content scheme, or 'class 1' and 'class 2' content. Industry associations are working to develop codes. If it is not possible for codes to be registered to apply to relevant sections of the industry, the eSafety Commissioner may make an industry standard.

The Act provides as a matter of regulatory policy that that there should be reasonable efforts that for each section of the online industry, an industry code is to be registered within 6 months of commencement (prior to 23 July 2022) or for there to be an industry standard in place within 12 months of commencement (23 January 2023).

Industry codes and standards will apply to participants of 8 key sections of the online industry including providers of: social media; email; messaging; gaming; dating; search engine and app distribution services, and internet and hosting service providers; manufacturers and suppliers of equipment used to access online services; and providers that install and maintain the equipment.

Restricted Access System (RAS) Declaration

Under the Act, the eSafety Commissioner may issue remedial notices to online service providers in respect of material that has been, or would likely be, classified R18+ or Category 1 Restricted under the National Classification Code. This includes: realistically simulated sexual activity between adults; high impact nudity; high impact violence; high impact drug use; and high impact language.

Under a remedial notice, the service must either remove the material (or cease hosting the material, in the case of hosting service providers), or ensure that it is subject to a Restricted Access System (RAS).

A RAS is a way of controlling access to certain material based on age. The purpose of a RAS is not to prevent access to age-restricted content, but to ensure access is limited to people who are 18 years and over.

Under the Act, a RAS declaration must be in place at all times from commencement. The new RAS will be established through a legislative instrument to be declared by the eSafety Commissioner. This new RAS will replace the 2014 declaration, which updated the initial RAS from 2007.

Services that will need to meet the requirements of a remedial notice will include social media services, designated internet services and relevant electronic services that provide access to material from Australia. Remedial notices will also apply to Australian hosting service providers who will be required to stop hosting the material or take reasonable steps to ensure access to the relevant material is limited in accordance with the RAS.

Abhorrent violent conduct material blocking scheme

The scheme provides new powers for the eSafety Commissioner to protect the Australian community by seeking to prevent the viral spread of terrorist and extreme violent material online.

The Act allows eSafety to request (through issuing a blocking request) or require (through issuing a blocking notice) internet service providers to block material that depicts, promotes, incites or instructs in abhorrent violent conduct. This power will only be used for time limited periods in circumstances where the eSafety Commissioner is satisfied that the availability of the material online is likely to cause significant harm to the Australian community.

Abhorrent violent conduct occurs when a person:

- Engages in a terrorist act.
- Murders another person.
- Attempts to murder another person.
- Tortures another person.
- Rapes another person.
- Kidnaps another person using violence or the threat of violence.

These powers under the Act are consistent with, and complement, the Commissioner's powers in the *Criminal Code Act 1995*, enacted by the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* following the Christchurch terror attacks (as noted above on page 3).

Information-gathering and investigative powers

The Act includes a new information-gathering power for the eSafety Commissioner to help unmask the identities behind anonymous online accounts, where this information is relevant to the operation of the Act.

The Act also provides investigative powers for the Commissioner to summon a person to attend before the Commissioner (or their delegate), or to provide documents or information to the Commissioner regarding cyberbullying, image-based abuse, cyber abuse and online content investigations.

Online safety education, awareness, research and support

The Government committed \$39.4 million over 3 years (2020-21 to 2022-23) in the 2020-21 Budget, and an additional \$29.2 million for online safety over 4 years (2021-22 to 2024-25) in the 2021-22 Budget. On top of previous investments, this brings the total commitment to keeping Australians safe online over 4 years to over \$125 million (2021-22 to 2024-25). Most of this funding is for online safety education, awareness, support, research and investigations into harmful

online content and conduct. It allows eSafety to fulfil its existing functions, perform additional functions under the new Act and meet an increase in demand for resources and support.

This funding includes a \$5.2 million awareness campaign to inform Australians of the new and strengthened schemes under the Online Safety Act and eSafety's role in administering these schemes. The campaign is scheduled to commence when the Act comes into force in late January 2022.

The Government also committed \$4 million in funding to eSafety over 3 years (2019-20 to 2021-22) under the Fourth Action Plan of the National Plan to Reduce Violence Against Women and Their Children. This funding is for eSafety to help equip Aboriginal and Torres Strait Islander women, and women with intellectual disabilities with specific tools and support to help protect themselves from technology-facilitated abuse. The final year of this funding (\$1.3 million) is included in the total \$125 million figure.

Young Australians Online Safety Advisory Council

On 15 December 2021, the Government announced a new Young Australians Online Safety Advisory Council which will report to Government including recommendations for addressing key online safety concerns.

The Council will commence in 2022 and will build on the Government's objective to improve youth representation in the development of policy that affects them.

Age verification Roadmap

In June 2021, in response to the House of Representatives Standing Committee on Social Policy and Legal Affairs' *Protecting the age of innocence* report, eSafety was asked to develop an implementation roadmap for a mandatory age verification regime to limit children's access to online pornography. eSafety's Age Verification Roadmap will explore whether, and how, it is possible to complement the RAS with a mandatory age verification regime for online pornography. The Roadmap will be presented to Government by December 2022.²

Australian Competition and Consumer Commission Inquiries

Digital Platforms Inquiry

In July 2019, the Australian Competition and Consumer Commission (ACCC) published its final report for the Digital Platforms Inquiry (DPI). The Final Report examined the impact of three types of digital platforms (search engines, social media and digital content aggregators) on competition in the media and advertising services markets and made a total of 23 recommendations to government. In considering the intersection of privacy, competition and consumer protections, the ACCC's recommendations included strengthening the *Privacy Act 1988* and the development of a digital platforms code of conduct to address disinformation. On 12 December 2019, the Government released its Response and Implementation Roadmap for the Digital Platforms Inquiry (DPI Roadmap), which outlined an implementation program.

Digital Platforms Services Inquiry 2020-2025

On 10 February 2020, the Government directed the ACCC to conduct an inquiry into markets for the supply of digital platform services, with interim reports to be provided to the Treasurer every six months until 2025. These reports focus on competition and consumer issues arising in a range of digital platform services. So far, the ACCC has released three interim reports dealing with issues including consumer choice of web browsers, app marketplaces and online private messaging services. A fourth report considering general online retail marketplaces (such as Amazon and eBay) is due to be provided to the Treasurer at the end of March 2022.

Australian Code of Practice on Disinformation and Misinformation

Arising from the DPI, the Government asked the Australian Communications and Media Authority (ACMA) to oversee the development of a voluntary industry code addressing disinformation and news quality.

In February 2021, the Digital Industry Group Inc. (DIGI) launched the Australian Code of Practice on Disinformation and Misinformation (Disinformation Code). Eight companies have signed up to the Code – Adobe, Apple, Facebook (now

² More information on eSafety's age verification consultation can be found on its website at: <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>

Meta), Google, Microsoft, Redbubble, TikTok and Twitter. These companies commit to implement measures to reduce the risk of harms that may arise from disinformation and misinformation on their platforms and to release an annual transparency report about their efforts under the Code.³

In June 2021, ACMA provided the Minister for Communications, Urban Infrastructure, Cities and the Arts with a report on the code development process, the adequacy of digital platforms' measures and the broader impacts of misinformation in Australia. The Minister is considering this report.

DIGI announced new governance arrangements and a mechanism to resolve complaints about possible breaches by signatories of their Code commitments on 11 October 2021. Signatories to the Code had previously committed to do this within six months of the commencement of the Code. DIGI will commence a review on the effectiveness of the Code in February 2022.

Privacy reform

The Attorney-General's Department is responsible for privacy policy. In addition to the broader review of the *Privacy Act 1988*, on 25 October 2021 the Government released an exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021. The Bill implements the Government's commitment to strengthen the Privacy Act, confirmed the Digital Platforms Inquiry report, by increasing penalties and enforcement measures, and enabling the introduction of a binding Online Privacy Code for social media services, data brokerage services and large online platforms. The exposure draft of the Bill sets out that the Online Privacy Code must (among other measures) require social media services to take all reasonable steps to verify the age of individuals who use the social media service.⁴

Proposed online defamation reform

The Attorney-General is responsible for defamation at the Commonwealth level. The Attorney-General's Department has actively participated in the current Stage 1 and Stage 2 defamation reform as a member of the Defamation Working Party (led by NSW), which is conducted with the support of the Meeting of Attorneys-General (MAG). In addition to its active participation in the MAG defamation reforms, the Attorney-General's Department is advancing reforms on defamation on social media. On 1 December 2021, an exposure draft of the Social Media (Anti-Trolling) Bill 2021 was released.

The proposed legislation will address the harmful impacts of defamatory comments made online. The legislation will protect Australians who operate or maintain a page on a social media service from potential liability for defamatory comments made by others. It will also allow individuals to determine whether defamatory comments were made in Australia, and if so, to obtain the originator's contact details to facilitate the commencement of defamation proceedings in an Australian court. Specifically, the Bill will:

- Modify the outcomes of the High Court's ruling in *Fairfax v Voller* to make clear that Australians who operate or maintain a social media page are not 'publishers' of defamatory comments made on their page by third parties, for the purposes of defamation law.
- Make clear that social media companies are publishers of content on their sites and can be held liable for defamatory comments by users.
- Establish a new scheme that allows aggrieved individuals to complain to a provider of a social media service about defamatory comments made by an anonymous user, and to obtain that user's contact details with consent.
- Provide a mechanism for the courts to issue an 'end-user information disclosure order' that will 'unmask' anonymous originators of defamatory content in appropriate circumstances.
- Incentivise providers of social media services to adopt and comply with these new 'unmasking' mechanisms by granting the provider conditional access to a defence from defamation liability where it establishes (and complies with) the complaints scheme, and complies with applicable end-user information disclosure orders.

³ More information including a copy of the Disinformation Code can be found on DIGI's website at: <https://digi.org.au/disinformation-code/>

⁴ More information on the Privacy Act review and the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 can be found on the Attorney-General's Department website at: <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>

G20 engagement

At the G20 Rome Summit in October 2021, leaders agreed to take forward work during Indonesia's 2022 G20 presidency to improve internet safety and counter online abuse, hate speech, online violence and terrorism, recognising the responsibility of digital service providers. The Department is leading Australia's contribution to this work in consultation with other agencies including the Department of the Prime Minister and Cabinet, Department of Industry, Science, Energy and Resources, the eSafety Commissioner, Department of Foreign Affairs and Trade, Department of Home Affairs and the Attorney-General's Department.

Australian Government's transparency and accountability requirements of social media platforms and online technology companies

Reporting under the BOSE

From 23 July 2022 (six months after the commencement of the Act), the eSafety Commissioner may require a provider or class of providers to report on their compliance with the BOSE. The Act provides the Commissioner with the power to issue a:

- Periodic report notice requiring an individual provider to report to the Commissioner on their compliance with the BOSE multiple times at regular intervals.
- Periodic report determination requiring each provider within a class of providers to report multiple times at regular intervals.
- Non-periodic report notice requiring an individual provider to prepare only a single report to be given to the Commissioner.
- Non-periodic report determination requiring each provider within a class of providers to each prepare a report to be given to the Commissioner.

The Commissioner may seek information about a provider's compliance with all or specified basic online safety expectations. The provider must prepare the report in the manner and form specified in the Commissioner's notice or determination, and give the report to the Commissioner either within the time period specified in the notice or determination, or such longer period as the Commissioner allows (but not less than 28 days).

A provider that fails to comply with such a notice or determination from the Commissioner may be subject to a civil penalty. In addition to a court ordered civil penalty, the Commissioner has access to other enforcement options, including formal warnings, infringement notices, enforceable undertakings and injunctions.

The Act also provides for the Commissioner to publish statements about the performance of service providers in meeting the Government's expectations. It is intended that the BOSE will provide information to Government about the level of harm occurring on services used by Australians and help to drive improvements in online safety practices by industry.

Disinformation Code transparency reporting

Under the Disinformation Code (outlined above on page 8), signatories must provide an annual transparency report to DIGI setting out their progress towards achieving the outcomes contained in the Code which are published on the DIGI website. DIGI published the first set of signatories' reports in May 2021.⁵

Online Content Incident Arrangement (OCIA)

The Department of Home Affairs is responsible for the OCIA. The OCIA was developed in response to the 2019 Christchurch terrorist attacks livestream and associated content. It outlines the responsibilities and communication flows between Government and industry when livestreamed or viral terrorist or violent extremist content is declared an Online Crisis Event by the eSafety Commissioner.

⁵ More information on the Disinformation Code transparency reporting, and copies of the platforms first reports can be found at: <https://digi.org.au/disinformation-code/transparency/>

Australian taskforce to combat terrorist and violent extreme material – mandatory annual reporting

Following the report of the Australian Taskforce to Combat Terrorist and Extreme Violent Material Online, digital platforms, internet service providers and Australian Government agencies responsible for implementing the recommendations outlined in the Taskforce report must submit annual progress reports to support Government consideration of progress in implementing these recommendations and actions.

The Department was responsible for overseeing this annual reporting until 2021 when responsibility transferred to the Department of Home Affairs.

Table of Attachments

Attachment	Title
A	Online harms summary table
B	Online harms coordination mechanisms DITRDC is involved in

Attachment A: Online harms summary table

Type of harm	Lead agency	Agencies with an interest	Current regulatory framework
Cyberbullying of an Australian child	DITRDC ⁶	eSafety	<i>Online Safety Act 2021 (OSA)</i> ⁷ <ul style="list-style-type: none"> Cyberbullying scheme Basic Online Safety Expectations (BOSE)
Cyber abuse of an Australian adult	DITRDC	eSafety	OSA <ul style="list-style-type: none"> Adult cyber abuse scheme BOSE
Non-consensual sharing of intimate images	DITRDC Home Affairs	eSafety Attorney-General's Department (AGD)	OSA ⁷ <ul style="list-style-type: none"> Image-based abuse scheme BOSE <i>Criminal Code Act 1995</i>
Harmful material: <ul style="list-style-type: none"> Class 1 material (refused classification) Class 2 material (X18+/Category 2 Restricted) Class 2 material (R18+/Category 1 Restricted) 	DITRDC	eSafety	OSA ⁷ <ul style="list-style-type: none"> Online content scheme BOSE Industry codes RAS (only R18+/Category 1 Restricted material)
Other harmful material that does not meet the threshold of class 1 or 2 material but is addressed in Terms of Service, including suicide and self-harm content (including promotion of eating disorders) & dangerous viral challenges	DITRDC	eSafety	OSA ⁷ BOSE
Trolling and volumetric attacks	DITRDC	eSafety	OSA <ul style="list-style-type: none"> <u>May</u> meet threshold for adult cyber abuse under the Act <u>May</u> be covered by the BOSE
Harmful online advertising	DITRDC	ACMA	Australian Association of National Advertisers Code of Ethics (self-regulatory code enforced by Ad Standards)
Misinformation & disinformation	DITRDC	ACMA Home Affairs DFAT AEC Department of Finance Department of Health	Australian Code of Practice on Disinformation and Misinformation (voluntary code)

⁶ Department of Infrastructure, Transport, Regional Development and Communications

⁷ This is currently covered by the existing online safety framework, including the *Enhancing Online Safety Act 2015* and Schedules 5 & 7 of the *Broadcasting Services Act 1992*. The OSA replaces comes into effect 23 January 2022 and replaces the existing framework.

Type of harm	Lead agency	Agencies with an interest	Current regulatory framework
Abhorrent violent material	Home Affairs	DITRDC eSafety AGD AFP State & Territory Policing	<i>Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019</i> OSA ⁷ <ul style="list-style-type: none"> • Abhorrent violent conduct blocking requests and notices • Online content scheme • BOSE • Industry codes and standards
Terrorist and violent extremist exploitation of the internet	Home Affairs	AFP AGD eSafety	<i>Criminal Code Act 1995</i> OSA ⁷ <ul style="list-style-type: none"> • Online content scheme • Industry codes and standards • Abhorrent violent conduct blocking powers
Child sexual abuse material	Home Affairs	AFP AGD National Office of Child Safety (in PM&C) eSafety	<i>Criminal Code Act 1995</i> OSA ⁷ <ul style="list-style-type: none"> • Online content scheme • BOSE • Industry codes
Use of a carriage service to menace, harass or cause offence	Home Affairs	AFP S&T policing DITRDC AGD	<i>Criminal Code Act 1995</i>
Online hate speech and racism	AGD	Australian Human Rights Commission Home Affairs AFP DITRDC eSafety	<i>Racial Discrimination Act 1975</i> <i>Criminal Code Act 1995</i> OSA <ul style="list-style-type: none"> • <u>May</u> meet threshold for adult cyber abuse under the Act • <u>May</u> be covered by the BOSE
Online defamation	AGD	DITRDC	State & Territory defamation laws ⁸
Misuse/breach of personal information by digital platforms	AGD	Office of the Australian Information Commissioner	<i>Privacy Act 1988</i> ⁹
Online scams	Treasury AGD	ACCC AFP S&T Policing Australian Fraud Prevention Centre	Scams - Australian Consumer Law (Schedule 2 of the <i>Competition and Consumer Act 2010</i>) Fraud and identity theft - <i>Criminal Code Act 1995</i> and others

⁸ AGD is currently consulting on the exposure draft of the Social Media (Anti-trolling) Bill 2021.

⁹ AGD is currently considering submissions on the exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021.

Attachment B: Online harms coordination mechanisms DITRDC is involved in

There is complementary work occurring across Government in the online harms space. To ensure consistency and alignment of work there are coordination mechanisms in place, with Cabinet as the primary and overarching mechanism.

The below list includes the coordination mechanisms the Department is involved in that touch on our portfolio work in the online harms space.

In addition to these mechanisms, we also engage regularly with counterparts in other departments and agencies.

Online safety

- **Agency Heads Committee on Online Safety (AHCOS):** DITRDC chairs AHCOS which brings together heads of agencies across the Commonwealth that are involved in or have an interest in online safety.
- **eSafety Advisory Committee:** The eSafety Commissioner chairs this committee that brings together key representatives from industry, government, civil society and academia.
- **Cyber Security and Safety Communication Working Group:** DITRDC and Department of Home Affairs chair this officer level meeting of commonwealth agencies' with equities in cyber security and cyber safety to promote greater visibility and coordination of media and communications activities in the online safety and security space.
- **Australian Centre to Counter Child Exploitation (ACCCE) Prevention Awareness Working Group:** The Australian Federal Police led ACCCE brings together subject matter experts from Commonwealth agencies, non-government organisations (NGOs) and industry representatives to ensure the ACCCE can meaningfully contribute to the protection of children in Australia and overseas from exploitation.
- **Preventing Terrorist and Violent Extremist Exploitation of the Internet (PTVEEI):** The Department of Home Affairs chairs this interdepartmental committee which discusses issues relating to online terrorist material. The group provides updates on key work across government relating to preventing terrorist material and updates on international engagement.
- **Cyber Security Band 3 Inter-Departmental Committee:** The Department of Home Affairs and the Department of the Prime Minister and Cabinet co-chair this committee, which primarily considers cyber security matters but is also updated on the Government's online safety agenda.

Information integrity

- **Electoral Integrity Assurance Taskforce:** The Australian Electoral Commission and the Department of Finance co-chair this taskforce which brings together relevant federal government agencies that provide advice to the Electoral Commissioner on matters that may compromise the integrity of elections, including malicious cyber activity, electoral fraud, foreign interference and disinformation.

Digital platforms market issues

- **ACCC Digital Platforms Services Inquiry:** The Australian Competition and Consumer Commission (ACCC) leads work on the Digital Platforms Services Inquiry. The Department meets with the ACCC regularly to discuss progress with, and issues being raised in the Inquiry. These meetings also discuss progress with implementing the Government's response to the ACCC's Digital Platforms Inquiry released in 2019.
- **Digital Technology Interdepartmental Committee meetings:** The Department of the Prime Minister and Cabinet chaired meetings brings together agencies to discuss implementation of the Government's Digital Economy Strategy. This includes discussions on promoting more effective coordination across government to address challenges of emerging digital issues, including platforms issues.