Australian Government
Department of Infrastructure, Transport,
Regional Development, Communications and the Arts

Submission

Senate Economics References Committee Inquiry into international digital platforms operated by Big Tech companies

March 2023

Table of Contents

Introduction

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (the Department) welcomes the opportunity to make a submission to the Senate Economics References Committee's (the Committee) Inquiry into international digital platforms operated by overseas-based multinational technology companies ("Big Tech").

The Department is responsible for a number of matters considered by the Committee's Issues Paper. This includes the provision of policy advice to the Government on digital platforms and services, online safety, and cultural policy. We also work closely with portfolio regulators, the Australian Communications and Media Authority (ACMA) and the eSafety Commissioner, to deliver the Government's digital policy objectives. Noting the multi-faceted nature of these issues, responsibility may sit across a number of portfolios. The Department works closely with other agencies both within the portfolio and across government to provide cohesive advice to the Government.

This submission focuses on matters within the Department's policy remit, relevant to the Committee's Issues Paper. However, it does not comment on competition or national security issues that might arise with digital platforms.

What is a digital platform?

At its most basic level, the online environment facilitates the exchange of social and economic information, which in turn enables a slew of interactions, services and functions across our society and economy.

Digital platforms and services are a sub element of the online environment and services provided by online service providers. Digital platforms are an essential pillar of the Australian economy and society. They facilitate social connections, and enable and support a range of industries, including news and entertainment, recruitment, e-commerce, travel and transportation.

Digital platforms include websites and apps that offer value to users based on the presence of other users or other classes of users. This can be distinguished from other digital services, where the value is derived from provision of the service itself. Examples of digital platforms include social and other connective media services (Twitter, various Meta services, LinkedIn), marketplaces (Amazon, eBay, Facebook Marketplace), and content aggregator services (YouTube, TikTok).

Digital platforms and services have provided great social, cultural, educational and economic benefits. They help us connect, mediate access to news and entertainment, drive online commerce, and deliver a wide range of data-driven products and services. They also deliver substantial efficiencies for businesses in reaching consumers, and for Governments in making services and information available to citizens.

The digital economy more broadly has the potential to deliver strong productivity gains. In 2020-21, Australians were more likely to have watched an online subscription service than live or recorded free-to-air television for the first time. The Australian subscription video on-demand market grew nearly fifty per cent in 2021, with estimated total earnings exceeding $2.4 billion.

Online harms experienced by Australians

There are a number of risks when engaging on digital platforms and services, which can give rise to a range of harms. Examples of some online harms experienced by end-users, which are addressed through regulatory frameworks administered by agencies in the Communications portfolio include:

- cyberbullying and cyber abuse
- non-consensual sharing of intimate images

- illegal content, including child sexual abuse material and abhorrent violent material
- exposure to harmful material, including suicide and self-harm content and dangerous viral challenges
- online hate speech and racism
- harmful online advertising
- dis- and misinformation
- misuse/breach of personal information by digital platforms
- online scams.

In addition, digital platforms and services have created issues for certain key Australian sectors. For instance, the ready availability of mass content produced in other countries on streaming services, particularly the United States, risks crowding out the voices of Australian storytellers. Australia's content and cultural sectors also face various issues in how cultural content is made accessible and visible on digital platforms' algorithmically-driven recommendation systems. In particular, the prominence of content on platforms and services can influence users' viewing choices, thereby impacting the success of Australian content. Furthermore, some sectors – such as the Australian gaming industry – are struggling to compete with large multi-national tech firms that are starting to dominate markets and stifling the economic viability of smaller Australian competitors.

No single regulatory framework can address the broad scope of harms and issues presented by digital platforms and services. Instead, a targeted approach to regulation is required which seeks to ensure that regulatory responses are cohesive across Government.

Online algorithms

Algorithms play an important role in how digital platforms and services operate and are playing an ever-increasing role in how information and content is targeted at users. The role of algorithms on digital platforms and services and, in particular, their role in the curation of social feeds or search functions is a growing concern.

The implications of the use of algorithms on digital platforms and online services is being considered across a range of portfolio policy areas including:

- dis- and misinformation
- ranking and search algorithms relevant to how news is served to consumers
- digital and media literacy initiatives
- social harm issues – including echo chambers, online hate speech, and social media feed curation
- discoverability of Australian screen and music content on streaming services
- general consumer harms, including algorithmic biases or discrimination.

Algorithms are essential to the operation of the digital world. They assist end-users find content that they are more likely to be interested in, generally based on their own personal tastes and content they had previously interacted with. For instance, algorithms are used to drive recommendations on content streaming platforms, travel booking websites and navigation apps. Search engines also use algorithms to provide results that are more likely to be useful or contextually relevant to specific end-users, based on previous search history, user location or demographic profiling.

However, there is the potential for algorithms to amplify the harms experienced online. This can include radicalisation, user exposure to content or messages they wouldn't have otherwise sought out, improper amplification of voices, messages or harms beyond what would ordinarily happen outside online environments, as well as ad targeting and erosion of privacy.

The Final Report of the House of Representatives Select Committee's Inquiry into Social Media and Online Safety raised concerns about the opaqueness of algorithms, which has the potential to heighten harms associated with them. The Committee was of the view that a statutory requirement for platforms to provide the details of how they are working to minimise harms caused by algorithms would increase transparency without compromising commercially sensitive information. The Department is developing advice to the Government about the Committee's findings.

The role that algorithms play in ensuring discoverability of Australian cultural content has also been considered in the context of the Government's recently announced National Cultural Policy, *Revive*: a place for every story, a story for every place (Revive). Revive notes the Government's commitment to ensure that Australian music remains visible, discoverable and easily accessible to all Australians. Discoverability of Australian music content on streaming platforms and services is vital for Australian artists that distribute their music online, and compete with internationally recognised artists both abroad, and even in Australia.

Noting the need for a consideration of algorithms to be aligned across Government, the Department has commenced preliminary work with other agencies to consider the type and scale of harms as a result of algorithmic use, as well as the current transparency levels of various algorithms.

Algorithms – role of regulators

Regulators, both within the Communications Portfolio and across Government, are in the process of considering the impact of algorithms across the rage of regulatory remits. For instance, the Digital Platform Regulators Forum, comprising the ACMA, the eSafety Commissioner, the ACCC, and the Office of the Australian Information Commissioner, is in the process of understanding the impact of algorithms as they intersect with their respective agency regulatory remits. The insights gathered by current portfolio regulators from this exercise will be vital in informing policy considerations in relation to algorithms going forward, both in a general sense but also in relation to specific regulatory requirements. The Department will consider these insights as it progresses work on understanding the impact of algorithms and potential regulatory responses.

Children's Safety

The *Online Safety Act 2021* (the Act), which commenced on 23 January 2022, provides important mechanisms to protect children and young people from experiencing online harms, and to prevent online harms before they occur.

The Act gives powers to the eSafety Commissioner, Australia's online safety regulator. The eSafety Commissioner is responsible for promoting online safety in Australia and administering complaints schemes under the Act, including for adult cyber abuse, child cyberbullying, image-based abuse, and illegal and harmful online content.

The Act's cyberbullying scheme includes the following elements:

- A complaints scheme where a person may make a complaint about cyberbullying material, which is material that is likely to seriously threaten, humiliate, harass or intimidate an Australian child (under 18 years). Generally, the complainant must have first reported the material to the relevant online service provider before reporting to eSafety.
- 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.

In addition to the child cyberbullying scheme, the Act empowers eSafety to provide a range of educational resources to support young people, and their parents and carers, to deal with the effects of child cyberbullying.

The eSafety Commissioner also supports and complements law enforcement efforts to counter online sexual exploitation of children by regulating online content, and setting standards and expectations for digital platforms to provide safe and lawful online environments. The Act empowers the eSafety Commissioner to prevent and respond to online child sexual exploitation through:

- **The Online Content Scheme**

  Under Part 9 of the Act, the Commissioner may investigate complaints about online content and act on 'Class 1' material no matter where it is hosted. 'Class 1' material is material that is, or would likely be, refused classification under the National Classification Scheme. Refused classification material cannot be sold, hired, advertised or legally imported in Australia, and includes child sexual abuse material (CSAM).

  The Online Content Scheme empowers the eSafety Commissioner to seek the creation of strengthened industry codes or to impose industry standards. The Act includes examples of matters to be dealt with by the codes or standards, including procedures for dealing with CSAM. The eSafety Commissioner is working with industry on codes development.

- **The Online Safety (Basic Online Safety Expectations) Determination 2022**

  The Act also includes a set of Basic Online Safety Expectations through a ministerial legislative instrument, which was registered on 23 January 2022. This instrument allows the eSafety Commissioner to require transparency reports from services on how they are meeting the expectations. Matters within scope of the Determination are consistent with the Act and the policy objective of keeping Australians safe online. As such, the expectations highlight the importance of minimising the extent to which certain content is available on a provider's service, including how platforms are preventing their platform from being used to access abuse material. Failure to respond to a reporting notice from the eSafety Commissioner can also attract a civil penalty.

  In August 2022, the eSafety Commissioner issued legal notices to seven online service providers – Apple, Meta, WhatsApp, Microsoft, Skype, Snap and Omegle – requiring them to provide information about their efforts to prevent CSAM on their services. In December 2022, eSafety published summaries of industry's responses, highlighting inadequate and inconsistent use of technology to detect CSAM and grooming, and slow response times when this material is flagged by users. In February 2023, eSafety issued further notices to Google, Twitter, TikTok, Discord and Twitch focussed on child sexual exploitation and abuse, sexual extortion and the safety of algorithmic recommendation systems.

The efficacy of the current online safety framework will be assessed through the legislated review of the Act. The Act includes a provision for an independent review of its operation, which must commence by January 2025. This review provides the appropriate mechanism to consider amendments to the existing framework as it allows time for any weaknesses in the Act to be properly assessed.

In addition, online safety is a global challenge that requires a collaborative and coordinated response. The review of the Act provides the appropriate mechanism to consider:

- the operation of the existing framework, including industry codes and the Basic Online Safety Expectations reporting regime
- emerging international regulatory regimes and approaches, including the proposed UK Online Safety Bill, Ireland's Online Safety and Media Regulation Act 2022, the EU Digital Services Act, as well as California's Age-Appropriate Design Code Act.

Future enhancements to online safety protections

Digital platforms have primary responsibility to create safe online spaces for their users, including children. As private businesses, online service providers are responsible for their users' safety, and are accountable for their users complying with their terms of service. However, the Australian Government plays an important role in holding industry to account and providing a safety net for when platforms fail to protect Australians.

In addition to the eSafety Commissioner's regulatory powers, the Australian Government funds measures to help protect children online, including online safety education and awareness, youth engagement, and ongoing work to respond to CSAM and young people accessing online pornography.

Online safety education

In the 2022-23 October Budget, the Australian Government committed $6 million over three years (2023-24 to 2025-26) to support the national rollout of digital and media literacy eLearning tools developed and delivered by the Alannah and Madeline Foundation. Together, the eSmart Digital Licence+ for students aged 10 to 14, the eSmart Media Literacy Lab for secondary students aged 12 to 16 and a new eSmart Junior Digital Licence+ for primary students aged 5-9 will be made freely available to every Australian school. These products will help Australian students develop the skills they need to be critical, responsible and active citizens online.

A core function of the eSafety Commissioner is to support, encourage, conduct, accredit and evaluate educational programs relevant to online safety. Within this remit, the eSafety Commissioner has delivered a range of resources to educate children, their parents and carers on preventing and responding to online harms. The eSafety Commissioner has also developed a Best Practice Framework for Online Safety Education and a Toolkit for Schools to support a nationally consistent approach to online safety education.

The eSafety Commissioner provides specific educational resources, teacher professional learning, education for parents and carers, and training for other professionals working with children and young people. The eSafety Commissioner also works with external providers to increase access to high quality online safety education in schools. The Trusted eSafety Provider program endorses providers of online safety education whose programs align with the Best Practice Framework and who are required to provide information about eSafety's reporting mechanisms in each program they deliver.

In December 2022, the eSafety Commissioner established the Online Safety Education Council to coordinate online safety education with 22 education authorities in states and territories to promote best practice and national consistency. The group will also raise awareness of reporting and support agencies, and provide opportunities for better coordination of responses to critical online safety issues.

Youth engagement

The Online Safety Youth Advisory Council, which is coordinated and managed by the eSafety Commissioner, is an important forum for Government to hear directly from young people on issues they experience online and ways of supporting them to have positive experiences online. The Council was appointed in April 2022 and

met throughout 2022 to discuss online safety issues facing young people. The Council will report to Government after its first 24-month term with any outcomes and actions identified by the Council, as well as a 12-month interim progress report.

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 Restricted Access System, which aims to limit exposure to age-inappropriate online content, with a mandatory age verification regime for online pornography. The Roadmap will be presented to Government by March 2023.[1]

Collaborative efforts in response to CSAM

The eSafety Commissioner and the Department engage in a number of collaborative measures to address CSAM.

International

eSafety is the Australian member of INHOPE, a global network of 50 hotlines that works to rapidly remove CSAM from the internet. Where the eSafety Commissioner is made aware of CSAM located in an INHOPE member country, eSafety refers the content to that country's hotline, alerting that country's law enforcement agency to the content for investigation.

The vast majority of content referred through INHOPE is removed in less than three working days. In the small number of cases where CSAM is hosted in a non-INHOPE member country, eSafety informs the AFP.

The Department also supports the Attorney-General's Department's (AGD) work on the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, announced by Five Eyes countries and six major digital industry companies in March 2020.

Domestic

Under the first phase of the National Strategy to Prevent and Respond to Child Sexual Abuse 2021-2030:

- eSafety has received $3 million in the 2021-22 Budget to deliver programs to help parents and families prevent online harms to children, including sexual abuse.
- The Department supports AGD's efforts to collaborate with the digital industry against offenders' exploitation of online platforms to commit crimes related to the sexual abuse of children.

The Department recognises the important work to investigate and disrupt online sexual exploitation of children by the Australian Federal Police, the Australian Border Force, Australian Transaction Reports and Analysis Centre, and the Australian Criminal Intelligence Commission. The Department and eSafety participate in forums chaired by the AFP-led Australian Centre to Counter Child Exploitation, including the Prevention Stakeholder Forum and the Research Working Group, which seek to coordinate efforts to address child exploitation across Government and the non-profit sector.

---

[1] 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

Disinformation

The Communications Portfolio, including regulators the ACMA and the eSafety Commissioner, has a range of levers that are used to counter the effects of dis- and misinformation and which contribute to a more trusted information environment. These levers include:

- support for high quality public interest journalism, e.g. through funding of ABC and SBS
- education programs to improve media and digital literacy in the community
- provision of reliable information including in languages other than English, e.g. SBS provided critical COVID-19 health information in 63 languages
- the ACMA, under the *Broadcasting Services Act 1992*, regulating news and journalism content on traditional radio and television broadcasting services
- new powers currently under development that will allow the ACMA to combat online dis- and misinformation.

As noted earlier, the Department is responsible for providing advice to the Government on a broad range of issues, and leads the development of policy and regulatory responses to ensure all Australians can connect to media and online services safely. This includes providing advice to the Government on disinformation, misinformation, and holding digital platforms accountable for harmful content on their services. The Department represents the Communications portfolio on the Electoral Integrity Assurance Taskforce and has policy oversight of the Australian Code of Practice on Disinformation and Misinformation (the Code).

The scale, complexity and impact of online harms requires coordinated responses and partnerships across Government. The Department engages extensively with other Government agencies, digital platforms, industry bodies such as the Digital Industry Group Inc. (DIGI), non-Government organisations and community groups to address these harms.

Current regulatory arrangements

In responding to the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry, in December 2019 the Australian Government requested that digital platforms develop a voluntary code of practice to address online dis- and misinformation and news quality concerns.

On 22 February 2021, industry group DIGI released the voluntary Australian Code of Practice on Disinformation and Misinformation, which has been adopted by 8 signatories: Adobe, Apple, Facebook, Google, Microsoft, Redbubble, TikTok and Twitter. The Code commits signatories to implement safeguards to limit the spread of dis- and misinformation on their platforms and to report annually on this commitment.

The ACMA's June 2021 *Report on the adequacy of digital platforms' disinformation and news quality measures* explored the question of whether the voluntary code meets community expectations. It made a number of findings and recommendations which have informed both DIGI's recently revised Code, released in December 2022, and the Government's decision to introduce new powers for the ACMA to combat dis- and misinformation on digital platforms.

Regulatory reform to hold digital platforms accountable

On 20 January 2023, the Hon Michelle Rowland MP, Minister for Communications, announced the Government's plan to provide the ACMA with new information gathering, record keeping, and reserve code registration and standard making powers to combat dis- and misinformation on digital platforms. These powers are consistent with the key recommendations in the ACMA's June 2021 report.

The ACMA powers will enable a graduated, needs-based regulatory architecture to strengthen and support the existing voluntary framework established by the voluntary code, and will extend to non-signatories of the voluntary code. The new ACMA powers will be focused on ensuring transparency around platform measures to combat dis- and misinformation, their effectiveness, and ensuring Government has avenues for regulatory intervention should industry self-regulation prove insufficient.

The legislation will be designed carefully to balance the public interest in combatting dis- and misinformation with the right to freedom of expression so fundamental to democracy.

European Union's Code of Practice on Disinformation

Governments around the world are grappling with how best to respond to dis- and misinformation on digital platforms. The European Union's (EU) 2022 Code of Practice on Disinformation,[2] like the Australian Code of Practice for Disinformation and Misinformation, is voluntary. Signatories can nominate which of the commitments they sign up to. The European Commission updated its voluntary Code of Practice on Disinformation in June 2022 (originally launched in 2018). Under the updated Code, signatories commit to action in several domains, including; demonetising the dissemination of disinformation; ensuring the transparency of political advertising; empowering users; enhancing cooperation with fact-checkers; and providing researchers with better access to data.

The EU Code will exist alongside the *Digital Services Act* which establishes a co-regulatory approach to managing dis- and misinformation online, with varying obligations for platforms depending on their size. Very large online platforms (VLOPs) will be obligated to mitigate risks relating to the spread of harmful content, including disinformation. Following the commencement of the *Digital Services Act*, the EU Code will have different purposes and enforcement remedies, depending on whether an organisation is a VLOP or another category of organisation.

Scams

The rise of digital platforms has contributed to the growth of online scams. Digital platforms and services are seen as a cost-effective way for scammers to efficiently reach a large number of end-users, and often with a high level of sophistication. Platforms and services can also inadvertently profit from scams occurring across their services, either directly through the sale of ad space for fraudulent products or services, or indirectly through commissions on apps and sales.

In its 2022 *Targeting Scams* report, the ACCC reported that nearly $1.8 billion in losses were reported to Scamwatch, ReportCyber, various financial organisations and other Government agencies in 2021. These losses are for scams occurring across telephony, SMS and email as well as digital platforms. Considering that around 30 per cent of scam victims are estimated not to report the scams they have fallen victim to, the estimated real loss of scams in Australia is thought to be well over $2 billion. For example, the ACCC believes the combined losses from scams may have reached as high as $4 billion in 2022. While online scams are currently responsible for a small proportion of the total losses from scams they are growing fast. Financial losses reported to Scamwatch from scams conducted via social networking and mobile apps for example are estimated to have almost doubled between 2020 ($49 million) and 2021 ($92 million).

Scams include a range of targets and vectors such as dating and romance scams, identity theft, unexpected money or winnings, threats and extortion, job recruitment, investments, charities, phishing, hacking, remote

---

[2] More information about the EU's Code of Practice on Disinformation is available from the EU's website at: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

access scams and attempts to gain personal information, e-commerce scams, and telephone and messaging scams. Put simply, anyone can be a victim of scams.

In response to the increasing threat of scams, the Australian Government has committed to introduce strengthened measures to combat scams, including by establishing a National Anti-Scams Centre. While implementation of this commitment is being led by the Treasury, elements fall within the responsibility of the Communications Portfolio.

The ACCC's Digital Platforms Services Inquiry (DPSI) has considered the harms associated with online scams on digital platforms. In its fifth interim DPSI report, it recommended the introduction of mandatory processes for digital platforms to prevent and remove scams from their services, including through the use of a notice and action mechanism and improved verification procedures. The Treasury is consulting on a possible Government response to the report and the Department is actively working with the Treasury and the ACMA to shape advice to the Government in relation to measures to address online scams.

International jurisdictions

United States

The United States has proposed requirements for digital platforms to provide data access to vetted independent researchers and the public.[3] Coupled with increased transparency obligations to provide specific data sets to relevant regulators, this could significantly increase the monitoring of social harms present on digital platforms.

In the algorithmic context, researchers and/or regulators may be able to get open source codes relevant to the algorithms used by digital platforms, allowing them to review opportunities for algorithms to propagate harms. However, such a proposal is not without its own issues. For instance, access to this data may not be as simple as uploading lines of code and may require the physical attendance of researchers to the servers where such data is held. This could significantly limit access to algorithmic data.

Platforms are also likely to require vetting of researchers and regulators before allowing access to their algorithms. This could hamper access and limit the ability of researchers to access data in a timely manner.

Europe

The Department is closely following Europe's (EU) approach to digital regulation. The EU's *Digital Services Act* (DSA), which came into force on 16 November 2022, is focused primarily on issues concerning security, policing and recruitment – however, it also mentions transparency measures for online platforms on a variety of issues, including the algorithms used for recommending content or products to users. The DSA will become directly applicable across the EU either fifteen months after it came into force, or from 1 January 2024, whichever comes later.

United Kingdom

The United Kingdom's (UK) *Online Safety Bill*, currently in the House of Lords, would place a range of duties to require providers of regulated user-to-user and search services to operate their service in a safe way, eliminating harmful and illegal content. The Bill is drafted in such a way that the relevant duties would take

---

[3] Section 4, Platforms Accountability and Transparency Act, accessed 16 February 2023.

account of various aspects of system design including the algorithms underpinning online service. Duties in the Bill would place a range of obligations on the relevant service providers, such as:

- duties to carry out content risk assessments for illegal content, including risk assessments for child users (for services likely to be accessed by children)
- duties to use proportionate systems and processes designed to address illegal content present on their services
- duties to protect children.

In 2021, the UK Parliament published a Report into the Economics of Music Streaming, which called for a "complete reset" of the streaming market. The original report raised concerns around a number of issues, including transparency and algorithmic curation. The Government committed to undertaking several workstreams in its response to the report. A follow-up report published in January 2023 has again highlighted these concerns and notes the lack of progress made by the transparency and data working groups.[4]

New Zealand

The New Zealand Government collaborated with a number of civil society stakeholders to implement the Algorithm Charter for Aotearoa New Zealand in July 2020.[5] The Charter is focused on the Government's use of algorithms. The Charter represents a commitment to carefully manage how algorithms are used by Government in New Zealand. It outlines the Government's aim to minimise unintended algorithmic bias and use the power of algorithms to ensure better service delivery to New Zealanders while maintaining public trust in their usage.

National Cultural Policy

The Department develops cultural policy to support key Australian content creative sectors such as screen, music and video games. As stated above, on 30 January 2023, the Australian Government released *Revive*: a place for every story, a story for every place – Australia's Cultural Policy for the next five years. Backed by $286 million in dedicated funding over four years, the intention of *Revive* is to change the trajectory of the creative sector, to deliver new momentum so that Australia's artists and arts workers, organisations and audiences thrive and grow, and arts, culture and heritage are re-positioned as central to Australia's future. The Department has a policy and program development and delivery role under the National Cultural Policy.

The Department's national cultural policy remit has a number of crossovers with Big Tech and other digital platforms and services. For instance, Pillar 5 of *Revive*, Engaging the Audience, introduces requirements for streaming services to ensure continued access to Australian screen content. It also commits to Government action to ensure Australian music is "visible, discoverable and easily accessible across platforms to all Australians".

Big Tech companies, including Amazon, Google and Apple, and other digital platforms and services, such as Netflix, Disney+ and Spotify, provide services that stream screen and music content and use algorithms to tailor content for users. Algorithms may hinder Australians' ability to access home-grown screen and music

---

[4] UK house of Commons Digital, Culture, Media and Sport Committee, *Economics of music streaming: follow-up*, https://committees.parliament.uk/publications/33512/documents/182096/default

[5] Algorithm Charter for Aotearoa New Zealand, https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter

content. In addition, Australia's video game industry faces significant competition from video game development studios that are backed by Big Tech companies.

Screen content streaming

Submissions to the National Cultural Policy consultation process highlighted the importance of discoverability of Australian screen content on streaming services. Various industry stakeholders, including production companies, state film bodies and screen industry groups, argued that new content needs to be available and discoverable in order to maximise cultural impact and supported discoverability reporting by streaming services. It is therefore likely that certain industry stakeholders, including some Australian content creators, would support algorithmic transparency and, potentially, oversight powers.

However, other stakeholders, such as the streaming services themselves, do not support regulation of discoverability. Streaming services argued that they will naturally adequately promote content they have commissioned, ensuring it is discoverable to audiences.

Music content streaming

It is likely that providing oversight powers to an existing regulatory body or establishing a new oversight body in Australia would be welcomed by Australian music content creators. In submissions to the National Cultural Policy consultation process key industry stakeholders, including peak bodies that represent and provide support to Australian artists, musicians, managers and workers, called for Government intervention to develop policy settings to facilitate, as a priority, an increase in the availability and discoverability of Australian music content on streaming services.

One streaming service, in their submission to the National Cultural Policy consultation process, urged that any definition of Australian content should be broad and flexible and that what is considered to be 'culturally valuable' should be based on the types of content that Australians are consuming.

There are crossover issues between algorithmic transparency, and discoverability and availability of Australian music on music streaming services. Through consultations with industry stakeholders on *Revive*, the Department will explore how Australian content can be more easily and readily accessed on music streaming services, including the role that streaming service algorithms play in accessibility and discoverability. Algorithmic transparency is also likely to be a priority for Australian music content creators as they aim to improve their revenue streams.

Video games industry

As part of the National Cultural Policy, announced on 30 January 2023, the Australian Government is supporting the digital games industry through:

- introducing a Digital Games Tax Offset to grow large-scale games development in Australia, supporting projects with budgets of more than $500,000
- providing $12 million to increase investment to support digital games developers and small and medium independent games studios with project budgets up to $500,000.

These initiatives are complementary and represent an integrated plan to support the whole of Australia's digital games sector.

News Media and Digital Platforms Mandatory Bargaining Code

The News Media and Digital Platforms Mandatory Bargaining Code (the Code) aims to help sustain public interest journalism in Australia by addressing bargaining power imbalances between digital platforms and news media businesses.

It does so by establishing a framework to incentivise digital platforms and news businesses to reach commercial deals. Where this fails, the Treasurer may designate a digital platform, initiating a process for good faith negotiation and (if required) binding arbitration.

The Code, which came into effect on 3 March 2021, is legislated under the *Competition and Consumer Act 2010* which is the responsibility of the Treasury portfolio. However, the Code's policy objectives to sustain public interest journalism and the stakeholders to which it applies sit with the Communications portfolio.

A statutory review of the Code, conducted by the Treasury in 2022 following its first year of operation, concluded it has been a success to date, with over 30 commercial deals struck between digital platforms and a broad range of news media businesses.

The review made several recommendations which the Government is currently considering.