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

Freedom of Information Request 25-073

Travel expenses to accompany the Minister for Communications in the UK and Europe in February 2024 for departmental staff and officials travelling from Australian posts in London and Europe

October 2024

This document provides details of expenses for non-ministerial staff accompanying the Minister for Communications during travel to the UK and Europe in February 2024. Specifically, this includes expenses for departmental staff and officials travelling from Australian posts in London and Europe where this information is held by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

Table 1: Expenses of identified staff and officials for travel to the UK and Europe in February 2024 to accompany the Minister for Communications.

Category	Secretary – Jim Betts	A/g First Assistant Secretary – Bridget Gannon	HOM Madrid – Sophia McIntyre
Airfares	$12,876.34	$16,801.84	Nil.
Other Transport	$625.24	$807.35	$886.49
Accommodation	$2,903.14	$5,475.41	$2,839.74
Meals	$871.55 (some expenses shared)		Nil.
Other costs	$183.30	$61.29	$489.67

Costs included are for staff whose purpose of travel was to support the Minister for Communications. Secretary Betts accompanied Minister Rowland to London and Brussels. A/g First Assistant Secretary Gannon accompanied Minister Rowland to London, Brussels and Barcelona. Ambassador McIntyre travelled from the Australian Embassy in Madrid to Barcelona to provide support for Minister Rowland. Officers personally bore the costs of all other expenses not included in the above table (e.g. meals and incidentals).

Pages 1–120 of Document 2 removed as irrelevant to the request under section 22(1)(a)(ii) of the FOI Act.

Daily Program - Friday, 23 February 2024

Local Time		AEDT
s22(1)(a)(ii)		
0830-1000 (starting at 0900)	**Panel Event hosted by Brussels Chapter of International Institute of Communication** (brief below) *Venue: Offices of McDermott Will & Emery, avenue des Nerviens 9/31, 1040 Brussels* *Introduction by: TBC* *Moderator: Ms Ana Fota, Politico* *Panel Members:* - *Minister Rowland* - *Dr Julie Posetti*	1830-1900
s22(1)(a)(ii)		

Page 122 of Document 2 removed as irrelevant to the request under section 22(1)(a)(ii) of the FOI Act.

Panel event hosted by Brussels Chapter of International Institute of Communication

Time and place	**Key attendees**
Friday 23 February 0830 for 0900 start *Offices of McDermott Will & Emery, avenue des Nerviens 9/31, 1040 Brussels*	Introduction by: TBC Panel Members: Minister Rowland Professor Julie Posetti, Global Director of Research at the International Center for Journalists Moderator: Ms Ana Fota, Politico Note: Media will attend this panel

Relevant Key Issues Briefs

2 Online Safety Act implementation and review

3 Misinformation and disinformation

5 AI (including copyright and online safety)

8 EU digital regulation

Talking Points [general]

Misinformation and disinformation

- The Australian Government is very alive to the threats that are posed by harmful misinformation and disinformation to the safety and wellbeing of Australians, as well as to our democracy, society and economy.
- The Australian Government supports a diverse and sustainable media sector. It recognises that quality news and public interest journalism play an important role in the functioning of Australian society and democracy, and are essential to informing local communities.
- Australia takes a holistic approach to address mis- and disinformation, including cross government engagement, media literacy, factchecking, content in languages other than English and developing the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill.
- The Australian Government has undertaken consultation on a draft Bill, which would provide the regulator, the Australian Communications and Media Authority, with new information-gathering, record-keeping, code registration and standard making powers in relation to misinformation and disinformation.
- I am considering a number of changes to the Bill based on feedback from the consultation including refinements to definitions, transparency and accountability, clarification on religious freedom, and improvements to workability of the Bill to ensure that it can be implemented by the platform industry prior to introducing in Parliament this year.

EU digital regulation

- The EU has undertaken ambitious and commendable work to introduce strong regulations for digital platforms, aimed at levelling the playing field for businesses and protecting consumers. The Australian Government has been closely monitoring developments in the EU, as we work towards achieving those same objectives for Australians.

AI

- The Australian Government recently published its interim response to consultation on Safe and Responsible AI. Our aim is to ensure the design and deployment of AI systems in Australia in legitimate, but high-risk settings, is safe and can be relied upon. At the same time, we want to ensure the use of AI in low-risk settings can continue to flourish. Areas identified for action include preventing harms from occurring through testing, transparency, and accountability measures; and clarifying and strengthening existing laws to safeguard citizens.
- The Australian Government is also working internationally to support the safe development and deployment of AI, including by taking forward the commitments in the Bletchley Declaration.
- The Minister for Industry and Science is leading Australia's efforts in this space.

OSA implementation and review

- Australia's *Online Safety Act 2021* came into effect in January 2022. Australia's online safety regulator, the eSafety Commissioner, has been successfully implementing the Act and addressing online harms.
    - In November 2023, I announced an independent review of the Act ensure our regulatory framework remains fit for purpose and responsive to emerging harms and technologies.
    - The review will look at what is happening internationally, including the European Union's Digital Services Act and the UK's Online Safety Act.
    - The report of the independent reviewer will be provided to Government in the second half of 2024, with implementation of any changes expected in 2025.

Questions [you may wish to ask]

- What are the main challenges in tackling misinformation and disinformation in the EU?

Talking Points [NEW]

What are some steps Australia has taken to tackle disinformation and misinformation, and what do you see as the biggest challenges we still face?

Australia takes a wholistic approach in tackling dis- and misinformation

- The growing use of online platforms has increased the spread of disinformation and misinformation and has become a significant challenge for governments.
- In Australia, we take a whole of society approach to combat this growing challenge, this includes:
    - educating Australians to critically engage with false and misleading information
    - responding to disinformation and misinformation with communication, regulatory or other activities, and
    - partnering with international and industry stakeholders.

Government and industry need to work together to increase transparency

- One major challenge is to determine the roles of government and the digital platforms in the regulation of content hosted on digital platform services.
- We've seen that, while there is a very important role for industry to play, this issue cannot be entirely left to the discretion of the digital platforms. The platforms have taken some actions, but these lack transparency and consistency.

- Given the serious societal harms caused by disinformation and misinformation there is clearly a role for government to hold digital platforms to account.

Australia is introducing new legislation that will empower online users

- The Australian Government has proposed draft legislation, which will provide our regulator, the Australian Communications and Media Authority (ACMA), with new powers to increase transparency and hold digital platforms to account and improve their efforts to combat harmful disinformation and misinformation.
- The ACMA would have information gathering and record keeping powers which will lift the hood on platforms' efforts and the effectiveness of our current voluntary code.
    - This will empower online users to better understand how their online content is managed by the digital platforms.
- If voluntary industry efforts fail, the ACMA would have reserve code registration and standard making powers to place obligations on the digital platforms to improve their systems and process such as complaints handling and support for fact checkers. This would bring consistency to the systems and process used across platforms.
- The ACMA would be empowered to obtain and publish information on how platforms are applying their terms of service and other related policies.
    - This will improve transparency and hold platforms accountable for the decisions they make.
- It would also enable Australian online users to make better informed choices about how they engage with these platforms.
- The graduated nature of the proposed ACMA powers and the focus on systems and processes, rather than specific pieces of content, is a key element of the proposed Australian framework.
- The draft Bill also includes a number of safeguards to protect freedom of speech and public debate, a challenge for Governments around the world when looking at interventions.
    - The ACMA will have no role in determining truthfulness, and it will not be able to require platforms remove particular pieces of content.
    - Importantly, it would not stop criticism of Government or stifle debate.
    - There are also explicit protections for freedom of communication. For example, when registering codes, the ACMA would be required to consider the effects on the freedom of political communication.
    - The framework would be open to regular system reviews and parliamentary oversight.
- Another challenge which policy makers face when designing regulation is that the regulation of disinformation and misinformation could be perceived as a form of government censorship or the establishment of a 'ministry of truth'. A careful balance is therefore required, between protecting from harms and preserving freedom of expression.
- The Australian Government has undertaken consultation on a draft Bill, and I am considering a number of changes to the Bill based on feedback from the consultation including refinements to definitions, transparency and accountability, clarification on religious freedom, and improvements to workability of the Bill to ensure that it can be implemented by the platform industry prior to introducing in Parliament this year.

Could you talk a little bit about how Australia is approaching this new challenge? How will Australia handle the rise of AI in the future?

Australia is committed to ensuring safe and responsible AI

- The Australian Government recently published its interim response to consultation on Safe and Responsible AI. Our aim is to ensure the design and deployment of AI systems in Australia in legitimate, but high-risk settings, is safe and can be relied upon. At the same time, we want to ensure the use of AI in low-risk settings can continue to flourish. Areas identified for action include preventing harms from occurring through testing, transparency, and accountability measures; and clarifying and strengthening existing laws to safeguard citizens.
- The Australian Government is also working internationally to support the safe development and deployment of AI, including by taking forward the commitments in the Bletchley Declaration.
- The Minister for Industry and Science is leading Australia's efforts in this space.

How does Australia work together with big tech companies such as META and TikTok to avoid the spread of disinformation and misinformation?

Government is working with industry to counter the spread of disinformation and misinformation online

- The Australian Government works with digital platforms including Meta and TikTok to counter the spread of harmful disinformation and misinformation online.
- Meta and TikTok are both signatories to the voluntary Australian Code of Practice on Disinformation and Misinformation. The Code commits digital platform signatories to reducing the risk of online disinformation and misinformation on their platforms in Australia.
- The Code was launched in February 2021 by industry group Digital Industry Group Inc. (DIGI) and has 8 signatories – Adobe, Apple, Google, Meta (Facebook), Microsoft, Redbubble, TikTok and Twitch. All signatories must commit to:
    - Reducing the risk of harms arising from disinformation and misinformation; and
    - Publishing an annual transparency report about the steps they are taking to combat disinformation and misinformation.
- The ACMA has oversight of the Code and reports on the adequacy of platforms' measures and broader impacts of disinformation and misinformation. The ACMA has published two reports on the adequacy of the Code and efforts of platforms disinformation and misinformation measures. The ACMA continues to engage with DIGI, code signatories and other relevant parties on the operation and review of the Code.
- The most recent ACMA report, published on 25 July 2023 found that while improvements had been made, there was room for further improvement regarding how signatories report their actions under the Code, the level of transparency around the measures, and the effectiveness of the measures.

Government and industry are working together on electoral integrity

- The Electoral Integrity Assurance Taskforce (EIAT) and Board, comprised of agencies across federal government, provides information and advice to the Australian Electoral Commissioner on matters that may compromise the real or perceived integrity of an Australian federal election or referendum.
- The EIAT works with digital platforms to ensure the integrity of electoral events, particularly from the spread of disinformation and misinformation.
    - For example, a number of EIAT Board members travelled to the United States in 2023 to meet with social media and technology companies in the lead-up to the Voice Referendum.
    - The delegation met with representatives from Amazon, Google, Meta, Microsoft, Open AI, Reddit, Tencent and X (formerly Twitter) to secure the support of the companies in ensuring

the integrity of the Referendum and seek updated points of contact for content referrals from the EIAT to platforms.

- There were also additional meetings held in Australia with Snap and TikTok.

- There is an enduring agreement between the Electoral Council of Australia and New Zealand (comprised of the Australian Electoral Commission and State and Territory electoral commissions) and online platforms for electoral events in Australia.
  - Google, Meta, Microsoft and TikTok are current signatories.
  - The agreement increases ongoing cooperation, establishes referral processes, provides points of escalation and facilitates briefings between platforms and electoral bodies.

Do you see a role for civil society and other private actors in combatting disinformation and misinformation?

Australia's holistic approach enables broad participation across society

- As I mentioned before, Australia takes a whole of society approach to ensuring information integrity and improving the health of the information environment.
- This illustrates the clear role that the Australian Government sees for civil society and the private sector in countering disinformation and misinformation.
- In the 2023-24 Budget the Government committed $2.5 million to support work in partnership with the Federation of Ethnic Communities' Councils of Australia (FECCA) to improve media literacy in vulnerable segments of culturally and linguistically diverse communities.
  - This funding will help address harms associated with the spread of disinformation and misinformation, as well as contribute to economic and civic participation in those communities.
- My Department also provides funding to the Alannah and Madeline Foundation to develop and roll out media and digital literacy products to all Australian schools, which will help students develop knowledge and skills to deal with digital challenges such as disinformation and misinformation.
- Independent fact checkers play a critical role in combatting the spread of misinformation and disinformation by verifying the accuracy of information encountered by Australians online and the authenticity of sources.
  - Several organisations currently provide this service in Australia, including the Australian Associated Press (AAP), RMIT ABC Fact Check and RMIT Fact Lab, and Agency France-Presse (AFP).

How can we make citizens across the world more resilient for online misinformation and the harm it causes, especially those in vulnerable positions? And how can we empower citizens to actively counter the flow of misinformation?

Government empowers all Australians to access high-quality information

- As mentioned, in Australia we take a holistic approach to improving the health of the information environment and ensuring Australians have the skills they need to counter the harmful impact of disinformation and misinformation.
- Governments are able to empower their citizens to develop their critical-thinking skills and abilities to help them discern manipulative content from trustworthy information.
- It is important for citizens around the world to have access to trusted, high-quality sources of news and information.
- In Australia, my Department has a range of policy levers available to respond to disinformation and misinformation and improve the integrity of the information environment. These include:

- Funding our national broadcasters, namely:
    - funding the ABC to provide high quality public interest journalism and Australian content for both Australian and international audiences.
    - funding the SBS to provide locally produced news and content to multicultural communities, and
    - SBS sharing critical COVID-19 and vaccination information in more than 63 languages.
- the ACMA under the Broadcasting Services Act 1992 regulates news and journalism content on traditional radio and television broadcasting services.
- education programs through the Office of the eSafety Commissioner and implementation of our election commitment to roll out the eSmart Digital Licence to equip Australians to better recognise potentially misleading information.
- undertaking work focused on media literacy, and supporting the sustainability and the diversity of the media sector and public interest journalism.
- the department is working to develop a News Media Assistance Program (News MAP) policy framework to assist the media sector to adjust to the modern media environment. The aim of this work is to develop an evidence base and framework to inform longer term measures to support public interest journalism and safeguard media diversity.

<u>As closely likeminded partners with strong shared values, what can Australia and the EU do together to more effectively combat disinformation and misinformation?</u>

- The European Union and Australia are both leading the way in shaping the regulation of online disinformation and misinformation.
- The Australian Government is committed to working with the EU on sharing insights on effective measures to counter the threats posed by disinformation and misinformation, particularly as they relate to regulatory measures.
- The sharing of key knowledge and insights on regulatory approaches to combatting disinformation and misinformation will ensure governments are able to strike the right balance between countering the harms of online disinformation and misinformation and upholding the freedom of speech and expression so fundamental to democracy.
- Australia is particularly interested in the EU's approach to transparency and its development of a performance measurement framework.
    - The EU experience will provide us with useful insights on developing key performance indicators and metrics to better understand the effectiveness of platform efforts to address disinformation and misinformation on their services.

Professor Julie POSETTI
Global Director of Research at the International Center for Journalists (ICFJ)
AUSTRALIA

Form of Address:	Professor Posetti, Dr Posetti
Education:	University of Wollongong, PhD, Journalism and Human Rights University of Canberra, Journalism
Social Media:	LinkedIn / Twitter

Professor Julie Posetti (PhD) is a multi-award-winning Australian journalist and academic based in Oxford (UK). At the International Center for Journalists (ICFJ) she leads a team producing research on contemporary crises and opportunities within the field of journalism. She is also Professor of Journalism at City, University of London.
Dr Posetti is the author of UNESCO's landmark global study, *Protecting Journalism Sources in the Digital Age*, which found that the legal frameworks to protect confidential journalism sources are outdated and inadequate. She is also the lead author or co-author/editor of the UNESCO reports *The Chilling: A global study of online violence against women journalists*; *Finding the Funds for Journalism to Thrive: Policy options to support media viability*; *Journalism, Fake News and Disinformation* and the UN Broadband Commission study *Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression*.
She has been published by the Washington Post, Foreign Policy, The Atlantic, CNN, BBC, ABC, the Sydney Morning Herald and others. Prior to joining ICFJ, Dr. Posetti was a Senior Research Fellow at the Reuters Institute for the Study of Journalism at the University of Oxford, where she led the Institute's Journalism Innovation Project.

Ana FOTA
Social Media Producer, Politico Europe
ROMANIA

Form of Address:	Ms Fota
English Ability:	Fluent
Education:	Fordham University, Journalism
Social Media:	LinkedIn / Twitter

Ana Fota is the social media producer for POLITICO Europe. Before moving to Brussels, Ana lived in New York, where she attended college and soon after became a news assistant for the New York Times, fulfilling a range of editorial duties that included reporting and running the social media accounts of various sections. While at the Times she published several pieces, including coverage of an amended museum display that sparked wide discussion online. She grew up in Bucharest and earned a B.A. in Journalism from New York's Fordham University, in 2018.

Pages 130–205 of Document 2 removed as irrelevant to the request under section 22(1)(a)(ii) of the FOI Act.

Key Issues Brief 2 – Online Safety Act Implementation and Review

Key Issues

- Australia's *Online Safety Act 2021* (the Act) came into effect in January 2022.
- Whilst the Act is relatively new, and has been successful in addressing online harms, you brought forward the independent statutory review of the Act to address gaps in the current framework and to respond to new and emerging harms and technologies.
    - On 22 November 2023, you announced the appointment of Ms Delia Rickard PSM to conduct an independent statutory review of the Act, with a period of public consultation. Public consultation will commence in the first half of 2024. Ms Rickard is expected to report back to Government in the second half of 2024. Implementation of any legislative amendments required as a result of the Government response to the review is anticipated to be in 2025.
- The review will consider the overarching policy objectives, the operation of the Act and the effectiveness of the complaints-based regulatory schemes.
- Holding the review this year will ensure the regulatory framework remains up-to-date and that the eSafety Commissioner can continue to keep Australians safe from online harms.
- Since the Act has come into effect, new online safety laws have been introduced across the globe, including in the European Union and the United Kingdom. The review will look at what's happening internationally, including what may be appropriate to adopt in the Australian context.

Industry codes and standards

- Industry is developing codes under the Online Content Scheme in two phases at the request of the eSafety Commissioner. The first set of codes address the most seriously harmful online content, such as child abuse material and pro-terror content.
- The codes development process commenced in late 2022 and currently six of the eight online industry sections have registered codes. The six registered codes cover social media services; internet carriage services; equipment providers (such as companies that provide smart devices to Australians); app distribution services; hosting services; and internet search engine services. All codes will commence six months following their registration in December 2023 or March 2024.
- If industry fails to meet a direction from eSafety to comply with an industry code, eSafety can take enforcement action (including seeking a penalty of up to $782,500 for a company).
- The Commissioner decided to not register the Relevant Electronic Services (RES) and Designated Internet Services (DIS) codes, and is moving to draft the standard.
    - On 20 November 2023, the Commissioner commenced public consultation on Phase 1 industry standards for RES and DIS providers.
    - RES are services that allow end-users to communicate with one another through email, instant messaging, SMS, chat services or online games (i.e. WhatsApp, Gmail, in-game chat).
    - DIS are services that allow end users to access material on the internet using an internet carriage service (websites and other online services).

- Other types of harmful content, such as less extreme types of Refused Classification material and online pornography will be addressed through a second phase of codes.
- The Commissioner is expected to commence work on the development of Phase 2 codes once the Phase 1 standards are finalised.

X Corp's legal proceedings for failing to comply with a reporting notice under BOSE

- In late 2023 X Corp was issued a penalty notice for failing to comply with a reporting notice, which was issued on 22 February 2023, on how it is tackling child sexual exploitation, sextortion and the use of algorithmic recommendation systems.
- On 10 November, Twitter (X) sought judicial review in the Federal Court in relation to the reporting notice and the issuing of the infringement notice.
- The Court has ordered X to file evidence by 19 January, and eSafety by 16 February, and has listed the proceeding for hearing on a date after 28 June 2024.
- On 21 December 2023, the eSafety Commissioner initiated civil penalty proceedings against X in the Federal Court regarding X's failure to pay the infringement notice. eSafety's intention is that the proceedings be held in tandem with X's judicial review application to facilitate speedy resolution of both matters.
    - As both the above judicial review and civil penalty matters are currently before the Court, it would not be appropriate to comment on either proceeding.

Notice to X Corp re hate speech

- A second report notice was issued to X in June 2023 asking for information on the steps it is taking to address online hate speech on its platform. eSafety found that X 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's capacity to address online hate on its platform, and that not enough is being done to tackle child sexual abuse material.
- X 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.

Complaints-based regulatory schemes

- The complaints-based regulatory schemes relate to child cyberbullying material, adult cyber abuse material, image-based abuse material, and illegal and restricted material.
- The key enforcement mechanism available to eSafety in response to a complaint is the issuing of removal notices to:
    - digital platforms to take down the relevant material, and
    - in some instances, the end-users who have posted or shared the relevant material.
- Generally, the recipient of a removal notice must remove the relevant material within 24 hours. Failure to comply with a removal notice carries a civil penalty of up to 500 penalty units ($782,500 for companies).

Basic Online Safety Expectations (BOSE)

- The Government recently concluded a period of public consultation on amendments to strengthen the BOSE Determination. Submissions closed on 9 February. The key reforms proposed include:

  - new additional expectations that generative artificial intelligence (AI) capabilities must be designed and implemented with user safety in mind and minimise the production of unlawful or harmful material;
  - that the best interests of the child should be front of mind in all actions taken by digital platforms;
  - detecting and addressing online hate speech that breaches a service's terms of use; and
  - the publication of regular transparency reports outlining what steps platforms are taking to keep Australians safe online.

- The BOSE Determination sets out the Government's basic online safety expectations for social media services, relevant electronic services (RES), and designated internet services (DIS).
- Service providers are expected to take reasonable steps to meet these expectations so that Australians can use their services in a safe manner and the Commissioner can issue legal reporting notices asking service providers to report against the expectations.
- While there are no penalties for service providers who do not meet the expectations, there are civil penalties of up to 500 penalty units ($782,500 for companies) for a failure to provide a report.
- As of 30 January 2024, the Commissioner has issued two separate reporting notices to online service providers on steps being taken to tackle child sexual exploitation and abuse, and one further reporting notice to X Corp in relation to online hate speech on its platform and the steps it is taking to minimize online hate and enforce its own policies against hateful conduct.

Key Issues Brief 3 – Misinformation and Disinformation

Key Issues

- The Government takes a holistic approach to address mis- and disinformation, including:
    - Developing the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill (the Bill) to be introduced in Parliament this year
    - Providing funding for our national broadcasters (ABC and SBS) to provide and distribute content in languages other than English
    - Providing $2 million to enable SBS to deliver additional independent journalism, in depth reporting and explainers, and expanding SBS's capacity to deliver accurate, balanced and impartial news in English and other languages
    - Supporting the Australian Electoral Commission's Disinformation Register and 'Stop and Consider' campaign
    - Establishing the Strengthening Democracy Taskforce in the Department of Home Affairs to build democratic resilience and respond to threats including disinformation
    - Engaging across our region and through our five eyes partners to counter the spread of mis- and disinformation
    - Providing $2.5 million to the Federation of Ethnic Communities' Councils of Australia to support media literacy in culturally and linguistically diverse communities
    - Maintaining an ongoing dialogue with digital platform service providers to promote the importance of their obligations and responsibilities to their users to manage and counter the spread of mis- and disinformation on their services.
- Industry also has an important role in tackling mis- and disinformation, including Digital Industry Group Inc (DIGI) administering the voluntary Australian Code of Practice on Disinformation and Misinformation (the Code).
- On 27 November 2023, DIGI announced it had withdrawn X's signatory status to the Code.
    - DIGI's independent complaints sub-committee upheld a complaint that before the Voice Referendum, X had removed mechanisms that allowed users to report mis- and disinformation to the platform, which is a key requirement under the Code.
    - As X did not take remedial action or cooperate with DIGI's investigation, its signatory status was withdrawn.
    - X was also removed as an active member of DIGI, having failed to pay membership fees, however has now been reinstated as a member of DIGI following payment.
    - X has not re-signed to DIGI's voluntary code which means X users instead will need to rely just on X's Terms of Service to understand how it will manage mis- and disinformation on its platform. It is likely that the only prospect for changing this outcome is the passage of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill through Parliament (expected to be introduced later this year).

Background

- In 2019, the Australian Competition and Consumer Commission (ACCC) released its Final Report into the Digital Platforms Inquiry and made several recommendations including that:

    - An independent regulator should be directed to monitor the voluntary initiatives of digital platforms to enable users to identify the reliability, trustworthiness and source of news content featured on their services.
    - Digital platforms should implement an industry code to govern the handling of complaints about disinformation, which could be registered with and enforced by a regulator.
    - In the event that a code was not developed, a regulator should introduce a mandatory standard.
- On 22 February 2021, DIGI released the Code. The Code was initially adopted by 8 signatories including Adobe, Apple, Facebook, Google, Microsoft, Redbubble, TikTok and X (no longer a member). It commits signatories to implement safeguards to limit the spread of mis- and disinformation on their platforms and report annually on this commitment.
    - On 7 February 2024, Twitch, an interactive livestreaming service for content spanning gaming, entertainment, sports, music and more, adopted the Code.
- On 25 June 2023, the Government released an exposure draft of the Bill, which would provide the Australian Communications and Media Authority (ACMA) with information gathering, record keeping and code and standard making powers in relation to mis- and disinformation.
    - The draft Bill will empower online users through greater transparency of how their online content is managed and provide a regulatory backstop if voluntary efforts of the platforms fail. It will also ensure that platforms have stronger systems and processes in places such as reporting tools and internal dispute resolution.
    - We received almost 24,000 responses to the consultation, including comments and 2,400 submissions, which ran from 25 June to 20 August 2023.
    - The Government will consider a number of changes to the draft Bill based on the consultation feedback including refinements to definitions, transparency and accountability, clarification on religious freedom, and improvements to workability of the Bill to ensure that it can be implemented by the platform industry.

Organisation for Economic Co-operation and Development (OECD)

- On 13-14 November 2023, the OECD held a conference in Paris to identify effective policy responses to the challenges that mis- and disinformation present for democratic countries. The conference brought together representatives from government, digital platforms, media and communications, academics and civil society.
- A series of panel sessions considered potential regulatory responses, including:
    - The need for a common framework to tackle disinformation and strengthen information integrity.
    - Identifying priorities for coordinating regulatory policy across governments.
    - The significance of Artificial Intelligence (AI) as both an enabler of and tool against disinformation.
    - The use of regulation in minimising the risks related to online and offline information spaces.
    - The role of effective information-sharing and regulation in unmasking foreign interference.
- The OECD will be releasing its 'Tackling disinformation: Strengthening democracy through information integrity' report in early 2024.

Other recent developments in the European Union

- In October 2023, the EU issued a warning to X over the volume of Israel-Palestine disinformation hosted on the platform.
- X withdrew from the European disinformation code in May 2023, but remains bound by its obligations under the Digital Services Act (DSA).

Pages 212–213 of Document 2 removed as irrelevant to the request under section 22(1)(a)(ii) of the FOI Act.

Key Issues Brief 5 – AI (including copyright and online safety)

Key Issues

- Artificial Intelligence (AI) technologies have the potential to bolster the Australian economy, create new industries and provide more inclusive and accessible services.
- To realise these benefits, Australians must have trust in the safety of AI applications developed by the private sector, governments and academia.
- On 17 January 2024, the Australian Government released its interim response on *Safe and responsible AI in Australia consultation*.
- The interim response balances the Government's objective to maximise economic and social opportunities from AI, while preventing possible harms through the deployment of this technology.
- Key focus areas for the Government include:
  - preventing harms from occurring through testing, transparency and accountability
  - clarifying and strengthening laws to safeguard citizens
  - working internationally to support the safe development and deployment of AI
  - maximising the benefits of AI

Online Safety

- The Australian Government is working on a range of online safety policy issues including the implementation of the Online Safety Act, hate speech, and age verification.
- The Online Safety Act (OSA) is agnostic about the way in which the content is created. Rather, it focuses on the harm arising from the content.
- The OSA includes complaints-based schemes to provide time-sensitive and victim-centred support for individuals. This approach is underpinned by transparency and accountability of online service providers.
- On 22 November 2023, Ms Delia Rickard PSM was appointed to undertake an independent review of the Online Safety Act 2021 (the Act).
- Public consultation on the review is expected to take place in early 2024 and the final report is expected to be delivered late 2024.
- The review will be broad-ranging and include consideration of the overarching policy objectives, and the operation of the Act.
- It will also examine the effectiveness of the complaints-based regulatory schemes, how it is addressing online harms, and identify gaps in the legislation.

Copyright

- The Attorney-General hosted four roundtables on copyright issues throughout 2022-23, including on 'Artificial Intelligence and Copyright'.
- Following the final roundtable on 4 December 2023, the Government established a copyright and AI reference group to provide a standing mechanism for ongoing engagement with stakeholders.

- The reference group will complement other AI-related Government initiatives, including the Safe and responsible AI work being led by the Department of Industry, Science and Resources (DISR).

International Telecommunication Union (ITU) mandate on AI

- Australia recognises ITU's role in developing telecommunications standards in support of AI (as outlined in the AI Resolution adopted at the 2022 ITU Plenipotentiary Conference). The AI Resolution instructs ITU to continue its efforts on AI related to telecommunications/ICTs:
    - conducting studies, and facilitating information-sharing and capacity building on AI technologies for increasing the efficiency of telecommunications/ICTs.
    - fostering a telecommunication/ICT ecosystem for deployment of AI technologies.
- ITU is not within its expertise or mandate to develop standards that relate to universal human rights, such as development of ethical AI algorithms.
- We are very cautious of non-likeminded proposals to expand ITU's mandate on AI into areas of ethics, human rights, privacy, cyber security and data protection.
- Expansion of this type would duplicate existing multilateral and bilateral efforts within the mandate and core competencies of other international bodies, including the OECD.
- We advocate for the development of AI technical standards to remain in expert-led, multi-stakeholder bodies such as the ISO and the IEC (rather than in the ITU which is controlled by governments — many of which are not likeminded with Australia on human rights, privacy, cyber security and related issues).

Background

Australian Government Response to AI (led by DISR)

- The interim response on *Safe and responsible AI in Australia* follows consultations led by the Department of Industry, Science and Resources (DISR).
- Over 500 submissions were received in response to the consultation process.
- DISR have established a number of cross-government working groups in order to progress this work.

Pages 216–219 of Document 2 removed as irrelevant to the request under section 22(1)(a)(ii) of the FOI Act.

Key Issues Brief 8 – EU digital regulation

Key Issues

- The EU's Digital Services Act package, consisting of the Digital Services Act (DSA) and the Digital Markets Act (DMA) came into force on 16 November 2022.
    - The DSA is intended to improve content moderation on digital platforms to address concerns about harmful and illegal content. The DMA is intended to place obligations and prohibitions on certain large digital platforms designated as "gatekeepers".
    - These Acts have extra-territorial reach. Given the global nature of the internet, it applies to service providers who are based outside of the EU but offer services to EU customers.
    - Under the DMA, the European Commission designated six gatekeepers in September 2023 – Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft. These companies must comply with their obligations under the DMA by March 2024.
    - Under the DSA, EU Member States will have to appoint Digital Services Coordinators by 17 February 2024, when platforms with less than 45 million active users will also have to comply with all DSA rules.
    - In December 2023, the European Commission opened formal proceedings against X to assess whether it has breached the DSA in areas linked to risk management, content moderation, dark patterns, advertising transparency and data access for researchers. This includes compliance with obligations to counter the dissemination of illegal content, and the effectiveness of measures taken to combat information manipulation on the platform. There is no legal deadline for bringing formal proceedings to an end.
- The European Union's Artificial Intelligence Act (AI Act) reached provisional agreement on 8 December 2023, after a long period of negotiations. The AI Act seeks to create a comprehensive legal framework for the regulation of AI systems across the EU, with the aim of ensuring they are safe and respect fundamental rights and EU values.
    - The AI Act adopts a risk-based approach, with the main focus being on unacceptable-risk and high-risk systems. Unacceptable-risk systems will be banned in the EU. These include biometric categorisation systems that use sensitive characteristics; untargeted scraping of facial images from the internet or CCTV footage; social scoring based on behaviour or personal characteristics; and emotion recognition in the workplace or educational institutions, amongst others.
    - High-risk systems, such as critical infrastructure, medical devices, systems to determine access to educational institutions or for recruiting people, will be subject to comprehensive mandatory compliance obligations.
    - Systems classified as limited-risk will be subject to more minimal transparency obligations.
- The European Parliament and Council has reached provisional agreement on a new regulation on 'European Union geographical indications for wine, spirit drinks and agricultural products'. Prominent examples of EU protected names include 'feta' cheese and 'kalamata' olives.
    - This proposal combines three existing regulations ((EU) 1308/2013, (EU) 2019/787 and (EU) 2019/1753), and introduces new powers, including protection for geographical Indications online.
    - If passed, it will require member states to disable European access to domain names infringing on registered geographical indications. This may impact Australian companies

who have registered domain names in order to sell wine, spirit drinks and agricultural products online.

- A different regulation (Regulation 2023/2411) on 'geographical indication protection for craft and industrial products' was passed on 9 October 2023. The original draft text of this regulation included similar domain name related provisions. However, this text was removed before the regulation was passed.

- The EU's Network and Information Security 2 (NIS 2) Directive came into force in 2023, expanding the scope of the EU's cyber security rules to new sectors and entities. Of particular interest are the obligations in Article 28 which require domain name registries and registrars to maintain and publish registration data, and provide data to law enforcement.
  - There is concern in the domain name industry that these rules will have extraterritorial reach. For example, if an EU resident creates a ".au" domain, the NIS 2 Directive may place obligations on the .au Domain Administration in Australia.
  - The 27 EU member states are currently transposing the NIS 2 into their national legislations. There are concerns that these rules may be implemented in different ways across the EU member states, creating varying and complex policy requirements. There is a risk that entities may choose to avoid this regulatory burden and associated compliance costs by ceasing operations in Europe.

Background

Digital Service Act

- The Digital Services Act (DSA) has three main objectives:
  - establish a powerful transparency and accountability framework for internet intermediaries;
  - ensure the safety of users of digital services; and
  - create a harmonized approach to content regulation.
- The DSA includes rules for online intermediary services, but the obligations applicable to different online players are scaled to match their role, size and impact in the online ecosystem.
- **Intermediary services** offering network infrastructure: Internet access providers, domain name registrars, including also:
  - **Hosting services** such as cloud and webhosting services, including also:
    - **Online platforms** such as social networks or online platforms allowing consumers to conclude distance contracts with traders, where they disseminate information to the public at the request of the recipients of the service.
- **Very Large Online Platforms** and **Very Large Online Search Engines** pose particular risks in the dissemination of illegal content and societal harms. Specific rules are foreseen for platforms reaching more than 10% of 450 million consumers in Europe.
- On 25 April 2023, the Commission designated 19 VLOPs and VLOSEs:
- Obligations for all providers of **Intermediary Services** include:
  - They must designate single points of contact for communication with the authorities and with the recipients of their service;

VLOPs			VLOSEs
AliExpress	LinkedIn	Stripchat	Bing
Amazon Store	Pinterest	XVideos	Google Search
AppStore	Snapchat		
Booking	TikTok		
Facebook	Twitter		
Google Maps	Wikipedia		
Google Play	YouTube		
Google Shopping	Zalando		
Instagram	Pornhub		

  - In the absence of an establishment in the EU, they must designate a legal representative in one of the member states where the provider offers its services; and
  - They must adopt rules on admissible content and content moderation that respect the recipients' fundamental rights and provide annual reports on their content moderation to the authorities.

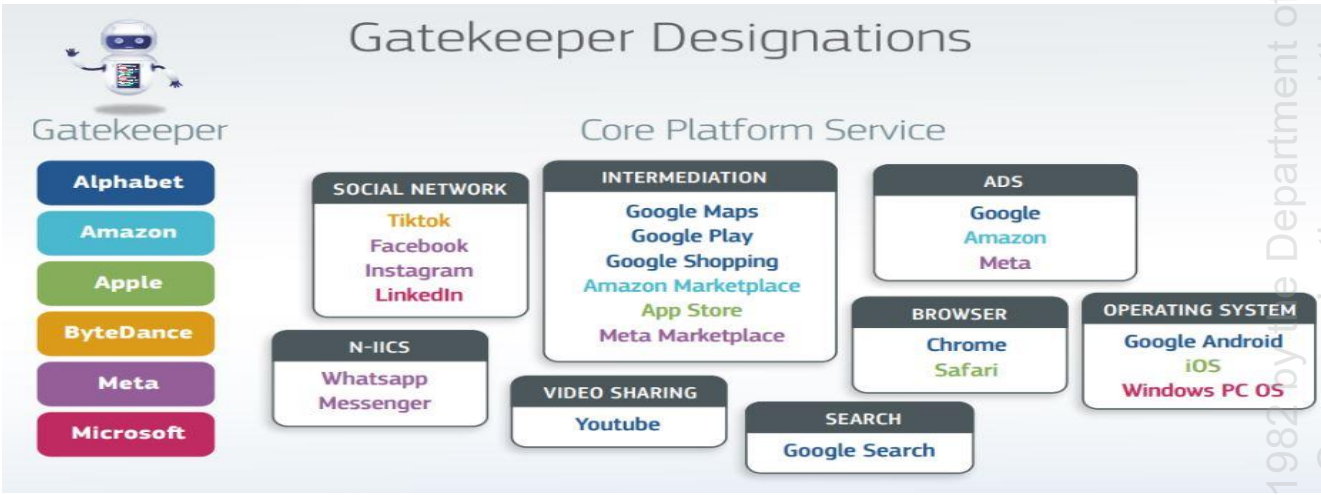
- Additional obligations for providers of **Online Platforms** include:
  - They must ensure a high level of privacy, safety, and security of minors; in particular, they must not present advertisements to minors based on profiling as defined in the GDPR;
  - They must have an internal complaint-handling system;
  - They must design and operate their online interface in a way that is not manipulative, deceptive (so-called "dark patterns"), or otherwise impairs users' ability to make free and informed decisions'
  - They must provide clear information on "each specific advertisement presented to each individual recipient," including "meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters"; and
  - They must provide information on any recommender systems in place in their terms and conditions.

Digital Markets Act

- The DMA applies to "**gatekeepers**" – designated as such by the European Commission, where they meet the following criteria:
  - (a) Has a significant impact on the internal market;
  - (b) Provides a **core platform service** which is an important gateway for business users to reach end users; and
  - (c) Enjoys an **entrenched and durable position** in its operations, or it is foreseeable that it will enjoy such a position in the near future.
- An undertaking is presumed to satisfy those criteria if it:

- For point (a), has either a turnover of at least 7.5 billion euro in the European Economic Area (EEA) in each of the last 3 years, or a market capitalisation or equivalent fair market value of at least 75 billion euro in the last financial year (FY).
- For point (b), provides a core platform service that in the last FY has more than 45 million monthly active end users in the European Union (EU), and at least 10,000 yearly active business users established in the EU.
- For point (c), the thresholds applying to point (b) are met in each of the last 3 financial years.

- Gatekeepers are the parent company. On 6 September 2023, the EU designated as gatekeepers Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft. Their 'core platform services' have been identified as follows:



Note N-IICS means number-independent interpersonal communication service.

- In addition to the core platform services above, the DMA lists cloud computing services and virtual assistants.
- Some services of companies that satisfy the gatekeeper thresholds have been determined not to be 'core platform services', such as Gmail, Outlook.com, and Samsung Internet Browser.
- After designation, the gatekeepers have 6 months to ensure full compliance with DMA obligations for each of their designated 'core platform services'.

Examples of "do's" – gatekeepers must:

- allow third parties to inter-operate with the gatekeeper's own services in certain specific situations;
- allow their business users to access the data they generate in their use of the gatekeeper's platform;
- provide companies advertising on their platform with the tools and information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper;
- allow their business users to promote their offer and conclude contracts with their customers outside the gatekeeper's platform.

Examples of "don'ts" – gatekeepers must not:

- treat services and products offered by the gatekeeper itself more favourably in ranking than similar services or products offered by third parties on the gatekeeper's platform;

- prevent consumers from linking up to businesses outside their platforms;
- prevent users from un-installing any pre-installed software or app;
- track end users outside of the gatekeepers' core platform service for the purpose of targeted advertising, without effective consent having been granted.

Pages 225–285 of Document 2 removed as irrelevant to the request under section 22(1)(a)(ii) of the FOI Act.