The Senate

Select Committee on Foreign Interference through Social Media

First interim report

December 2021

Printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra

Contents

Members

Chair
Senator Jenny McAllister — ALP, NSW

Deputy Chair
Senator Jim Molan AO DSC — LP, NSW

Members
Senator Sarah Hanson-Young — AG, SA
Senator David Van — LP, VIC
Senator Kimberley Kitching — ALP, VIC

Secretariat
Ms Lee Katauskas, Committee Secretary
Ms Fattimah Imtoual, Principal Research Officer
Dr Adrienne White, Senior Research Officer
Ms Ella Ross, Administrative Officer

PO Box 6100
Parliament House
Canberra ACT 2600

Telephone: (02) 6277 3585
Fax: (02) 6277 5794
Email: foreigninterference.sen@aph.gov.au

Abbreviations and acronyms

ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
AEC	Australian Electoral Commission
AFP	Australian Federal Police
AI	artificial intelligence
AMAN	Australian Muslim Advocacy Network
API	Application Programming Interface
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASPI	Australian Strategic Policy Institute
CCP	Chinese Communist Party
CFI	Countering Foreign Interference
CIB	coordinated inauthentic behaviour
CT	counter terrorism
CVE	Countering Violent Extremism
DFAT	Department of Foreign Affairs and Trade
DIGI	Digital Industry Group
DITRDC	Department of Infrastructure, Transport, Regional Development and Communications
DPI	Digital platforms inquiry (2017-2019, undertaken by the Australian Competition and Consumer Commission)
EIAT	Electoral Integrity Assurance Taskforce
Electoral Act	*Electoral Act 1918*
EU	European Union
FITS	Foreign Influence Transparency Scheme
ICES	International Cyber Engagement Strategy
JSCEM	Joint Standing Committee on Electoral Matters
MLAT	Mutual Legal Assistance Treaty
NCFIC	National Counter Foreign Interference Coordinator
NMRC	University of Canberra's News and Media Research Centre
OAIC	Office of the Australian Information Commissioner
ONI	Office of National Intelligence
PM&C	Department of Prime Minister and Cabinet
PRC	People's Republic of China
Privacy Act	*Privacy Act 1988*
The Taskforce	The Electoral Integrity Assurance Taskforce
QUT	Queensland University of Technology
SBS	Special Broadcasting Service
UK	United Kingdom

URL	Uniform Resource Locator (a web address)
US	United States of America

Recommendations

Recommendation 1

1.38 The committee recommends that the Australian Government clearly delegate lead accountability for cyber-enabled foreign interference to a single entity in government.

Recommendation 2

1.42 The committee recommends that the Australian Government take a proactive approach to protecting groups that are common targets of foreign interference but are not classified as government institutions.

Recommendation 3

1.45 The committee recommends that the Australian Government establish appropriate, transparent, and non-political institutional mechanisms for publicly communicating cyber-enabled foreign interference in our elections and review the processes and protocols for classified briefings for the Opposition during caretaker with respect to cyber-enabled foreign interference.

Recommendation 4

1.48 The committee recommends that the Australian Communications and Media Authority's report into the functioning of the Australian Code of Practice on Disinformation and Misinformation be publicly released as a matter of priority.

Recommendation 5

1.50 The committee recommends that the Australian Government publicly release the Electoral Integrity Assurance Taskforce's terms of reference.

Recommendation 6

1.53 The committee recommends that the Australian Government establish clear requirements and pathways for social media platforms to report suspected foreign interference, including disinformation and coordinated inauthentic behaviour, and other offensive and harmful content, and formalise agency remits, powers and resourcing arrangements accordingly.

Recommendation 7

1.56 The committee recommends that the Election Integrity Assurance Taskforce undertake an audit to assess capability relevant to detecting disinformation

prior to the coming election and, further, that the Australian Government consider providing information about relevant capabilities and resourcing to this committee as appropriate to assist in our deliberations.

Chapter 1
Committee view and recommendations

Context and objectives of this inquiry

1.1 Over the coming years, Australia will have to grapple with some big policy questions. How do we respond to climate change? Where will we find our future sources of shared economic prosperity? What role should we play in our region?

1.2 These are not easy questions. They ask us to consider what type of a nation we want Australia to be. Our best chance of finding good answers lies in leveraging our collective capacity for informed and inclusive public discussion. These discussions can be difficult to have at the best of times. They are next to impossible, however, if our digital public squares are crowded with disinformation and populated by inauthentic actors.

1.3 This senate inquiry was initiated following experiences in other democratic jurisdictions that showed what such a scenario may look like. Public inquiries into the conduct of the 2016 United States Presidential Election and the 2019 United Kingdom General Election showed some of the ways foreign (or foreign backed) actors, states and groups can use social and digital media to interfere with democratic discourse and election processes.

1.4 It would be naive to imagine that Australian elections and public debates have not, and will not, be the subject of similar attempts. The policy challenges facing Australia over the coming years are of interest to more than just Australians. There are a range of foreign governments, organisations and individuals who stand to win or lose from Australia's political and policy decisions. Experiences from overseas show us there are some foreign actors who also seek to introduce discord and social conflict as an aim unto itself. Technological developments mean that these actors have more options available than ever before to influence Australia's processes.

1.5 This present inquiry is not an investigation into the conduct of previous Australian elections—that task remains the responsibility of the Joint Standing Committee on Electoral Matters (JSCEM). Neither is it intended to be a definitive and exhaustive statement of the problem—much of the material the committee would need to undertake this task is not in the public domain, and the material that is available is subject to constant revision and revelations.[1]

[1] For example, just in the month prior to this report being finalised new information surfaced regarding the operations of Clearview, and there was reporting from a trove of leaked internal Facebook documents. It seems possible, if not probable, that further revelations about various platforms will come to light that augments our understanding of their operations.

1.6 Instead, this inquiry seeks to undertake a point-in-time assessment about the key risks posed by foreign interference via social media and the headline responses available.

1.7 This interim report sets out the evidence received from stakeholders about the nature of the problem facing Australia. It makes recommendations about the key steps government should urgently consider to enable our policy infrastructure to respond to the challenge in light of the impending federal election.

1.8 This report includes summaries of the evidence received about the motivations for foreign interference, the forms that it can take, the elements of social media platforms and their usage that foreign interference attempts often seek to exploit, and the social and cultural features that foreign interference attempts interface with. The committee will be calling for further submissions about the policy responses regarding social media platforms and users, civil society, news media and the information environment. Further consideration of these policy responses and relevant recommendations will be the subject of a future report by this committee.

The nature of the threat to Australian democratic processes

1.9 There has been considerable media coverage and public discussion of foreign interference efforts affecting other western democracies. It is natural for Australians to wonder: have we also been the subject of a concerted foreign interference attempt via social media?

1.10 The JSCEM concluded that there was 'limited evidence of social media manipulation within Australia, including minimal use of bots'[2] during the 2019 election. The Australian Strategic Policy Institute (ASPI) observed some examples of cyber enabled foreign interference that justified Australia's inclusion in its 2020 report on the issue.[3]

1.11 The Department of Home Affairs noted that it regularly observes 'campaigns unfolding on social media that involve disinformation'.[4] Some have been linked to foreign state actors:

> In 2017, following a terrorist attack in Brighton, Melbourne, the Department identified Tweets associated with accounts that have since been publicly attributed by Twitter to a foreign government entity.
>
> In another Australian example from 2017, accounts linked to the same foreign government entity were involved in discussions related to a plot to bomb an Etihad airlines flight departing Sydney International Airport. One

[2] Joint Standing Committee on Electoral Matters (JSCEM), *Report on the conduct of the 2019 federal election and matters related thereto*, December 2020, p. 122.

[3] See 2.13 and following in this report.

[4] Department of Home Affairs, *Submission 16*, p. 7.

> account used the disrupted plot to promote and amplify the hashtags "#MuslimBan" and "#StopImportingIslam". In this instance, hostile foreign state actors used social media to interfere in Australia's public discourse and attempt to undermine social cohesion.[5]

1.12 Submitters to this inquiry did not contend, however, that Australia had been the target of any large-scale, coordinated attempts.

1.13 This committee strongly believes that this is not a reason for inaction.

1.14 It is possible, if not likely, that Australia will face such an attempt in the future.

1.15 An explanation of the mechanisms by which foreign interference can be undertaken using social media is set out in chapter 2 of this report. In short, however, as Dr Wallis from ASPI noted:

> Authoritarian states have identified influence operations as a cheap yet effective mechanism for influencing and weakening liberal democratic societies and regional alliances.[6]

1.16 Foreign interference is more complex than just trying to boost one candidate over another in an election. Submitters to this inquiry spoke of a range of actors trying to do a range of things: actively sowing misinformation about particular issues, trying to inflame existing social divisions, or just creating a general environment of distrust.[7]

1.17 The consequences for Australia of a serious attempt could be severe in ways that are difficult to predict. Even a clumsy, unsophisticated effort runs the risk of undermining our ability as a nation to have the public discussions we need to deal with complex issues. As seen in other jurisdictions, it is enough to question the authenticity of a result for confusion and disunity to follow.

1.18 This committee believes that government should adopt an approach analogous to the precautionary principle in preparing to meet this challenge.

1.19 Waiting for a serious attempt before acting would be a mistake. Examples from overseas show that malign actors often seek to exploit existing social fissures or hot-button issues. A serious, concerted attempt at foreign interference could involve the amplification or manipulation of views that already have a domestic audience. It is not inconceivable that some Australian companies, organisations or even domestic political actors could believe that they may benefit from the relevant social media activity and so become unwitting participants in a foreign interference campaign. All of this would make mounting an effective response in real time challenging.

---

5 Department of Home Affairs, *Submission 16*, p. 7.

6 Dr Jake Wallis, Senior Analyst, International Cyber Policy Centre, Australian Strategic Policy Institute (ASPI), *Committee Hansard*, 22 June 2020, p. 10.

7 See 4.2 and following of this report.

1.20 This committee believes that government must approach the problem of foreign interference through social media with urgency and seriousness in order to create the institutional architecture needed.

1.21 Unfortunately, the government's actions so far have fallen short of this.

The adequacy of Australia's response to the challenge

1.22 Experts have been clear that what is required is a coordinated, cohesive response.

1.23 Ms Katherine Mansted told this committee:

> … we need a coordinated approach, we need a strategic approach and we need one that blends issues of domestic and foreign policy, issues of traditional security and non-traditional security …
>
> I think that what matters most is having a body that has the ability to look through multiple different sides of this problem, is resourced to do so and has both the informal and formal authority to take that step. This isn't just a national security problem either; it is also an economic problem.[8]

1.24 No such body has been established.

1.25 Nor has the government developed a coordinated approach. The committee was concerned by the convoluted answer to a simple question: who is in charge?

> CHAIR: Mr Hawkins, do you consider that Home Affairs is in the lead for policy development on disinformation and misinformation?
>
> Mr Hawkins: My area, at least, is in the lead for countering foreign interference. Disinformation and misinformation do not necessarily need to be foreign interference. They could be domestic. Our interests—
>
> CHAIR: Let me be more specific, then, Mr Hawkins. Are you the policy lead for foreign interference through digitally enabled, cyber, foreign interference?
>
> Mr Hawkins: Cyber is another area. We have a cyber team here, but there's the Australian Cyber Security Centre. We have our Ambassador for Cyber Affairs, who's here as well. But we're not responsible for the cyber elements, no.
>
> CHAIR: No, but for disinformation and misinformation that would constitute foreign interference, you are the policy lead?
>
> Mr Hawkins: If it's foreign interference, if it's a foreign actor and accords with those three, then, yes, we would be.[9]

---

8 Ms Katherine Mansted, *Committee Hansard*, 22 July 2020, p. 19.

9 Mr Neil Hawkins, Acting Deputy Coordinator and Acting First Assistant Secretary, National Counter Foreign Interference Coordination Centre, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 3.

1.26 The end result is that departments and officials are not across the work that is happening internally.

1.27 For example, the First Assistant Secretary of the Department of the Prime Minister and Cabinet's National Security Division was unaware that the COVID-19 taskforce was undertaking work to combat online disinformation and misinformation:

> CHAIR: Were you not aware of that process, Mr Colquhoun?
>
> Mr Colquhoun: I may have seen a product of it somewhere, but, other than that, I'm not involved at all, no.
>
> CHAIR: And not aware of it?
>
> Mr Colquhoun: No.[10]

1.28 Officials from the Department of Home Affairs (the supposed policy lead) were not aware which platforms were supposed to report foreign interference attempts to:

> CHAIR: I'm thinking about the somewhat proactive stance that's been taken by, for example, Facebook and Twitter in identifying coordinated inauthentic activity on their platforms. They publish regular reports about it. If they identify coordinated inauthentic activity that they attribute to a foreign state actor in the Australian context targeted at Australians, who do they talk to?
>
> Mr Hawkins: I'm not aware. I don't think they would talk to us. They may talk to the Australian Cyber Security Centre, but I couldn't answer that point.[11]

1.29 The platforms themselves were confused as well. Representatives from TikTok did not know if they were required to report any coordinated foreign interference attempts that they detected on their platform, let alone who they could even report this to. This is unsurprising given that, at the time TikTok appeared before the committee, the government had never contacted them about their expectations.

> CHAIR: Mr Thomas, do we know who we would notify if we saw something happening?
>
> Mr Thomas: I expect that would be some combination of DFAT, the Defence and the department of communications.
>
> CHAIR: But no request has been made of you, or no clear instruction has been provided, about who to notify and under what circumstances?
>
> Mr Thomas: That's correct.[12]

---

[10] Mr Lachlan Colquhoun, First Assistant Secretary, Department of the Prime Minister and Cabinet, *Committee Hansard*, 11 December 2020, p. 3.

[11] Mr Hawkins, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 5.

[12] Mr Brent Thomas, Director of Public Policy, Australia and New Zealand, TikTok Australia, *Committee Hansard*, 25 September 2020, p. 12.

1.30 Members of the committee have examined the aims of the relevant peak documents of the Departments of Home Affairs, Foreign Affairs and Trade, Defence, and other relevant agencies and consider that there is little cohesion in how they are written and limited interaction between them.

1.31 There is also no published strategy for combatting foreign interference via social media. Australia's Counter Foreign Interference Strategy is five dot points and six supporting sentences on a webpage.[13] There is nothing specific relating to foreign interference via social media.

1.32 Existing institutions for bringing together agencies to address foreign interference are unfortunately limited in scope. The Election Integrity Assurance Taskforce has answers to relatively simple questions, such as who should respond to a disinformation campaign about the electoral process. Its evidence to the committee showed it less able to answer more complex questions.

1.33 For example, it is not clear who is responsible for responding to a disinformation campaign that targets the information environment in an election period. A campaign of this kind could involve social media activity that attacks certain issues or particular participants such as unions, political parties, industry associations or ethnic groups. The Department of Home Affairs told the committee that responding to this would be the role of the Australian Electoral Commission (AEC); however, the AEC does not believe its legislation provides any basis for responding to such a campaign.

1.34 Likewise, the Taskforce does not seem to have been requested by the government to develop a clear framework to guide any response to foreign disinformation campaigns during the formal election period. The uncertainty about how the response to a disinformation campaign would interact with caretaker obligations is central to this. The decision to reveal or conceal evidence of a foreign-backed disinformation attempt is one that could have enormous implications during an election campaign. Both the Department of the Prime Minister and Cabinet and the Department of Home Affairs told the committee that while it was open to the Minister to brief the opposition, there was no obligation to do so under the caretaker conventions.

1.35 The committee believes this is not an acceptable state of affairs. Creating space for partisan decision-making about disinformation creates vulnerabilities in our institutional arrangements that malign foreign actors could exploit.

1.36 Transparency about the operations of institutions like the Election Integrity Assurance Taskforce would be an important first step. However, key aspects

[13] See Department of Home Affairs, 'Australia's Country Foreign Interference Strategy', https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-strategy (accessed 7 December 2021).

of the Taskforce are hidden. The functions and operations procedures are unclear even to its own members. There is a lack of certainty about responsibilities. Although the members can articulate their qualifications to be on the taskforce (for example, the Department of Communications is an expert on the social media platforms), there is no certainty about what their responsibilities and powers are, let alone the powers of others. The Taskforce is governed by terms of reference that have been kept secret to this committee and the public at large.

Next steps

1.37 Government needs to prioritise building the institutional architecture needed to respond effectively and proactively to the threat of foreign interference.

Recommendation 1

1.38 The committee recommends that the Australian Government clearly delegate lead accountability for cyber-enabled foreign interference to a single entity in government.

1.39 The committee notes the testimony of Dr Michael Jensen, referencing the comments made in the Australian Security Intelligence Organisation's Annual report for Financial Year 2020-21, which stated that 'based on current trends, we anticipate that espionage and foreign interference will supplant terrorism as Australia's principal security concern over the next five years.'[14]

1.40 Foreign interference is increasingly occurring online. ASPI's report on Cyber enabled foreign interference in elections and referendums found that 'the use of cyber-enabled techniques to interfere in foreign elections and referendums has increased significantly.'[15]

1.41 Australia is not immune from this challenge. Dr Jake Wallis and Mr Thomas Uren's submission to the committee noted that '[d]uring the 2019 Australian federal election financially-motivated actors from Kosovo, Albania and the Republic of North Macedonia used nationalistic and Islamophobic content to target and manipulate Australian Facebook users.'[16]

---

[14] Australian Security Intelligence Organisation, *2020-21 Annual Report*, 19 October 2021, p. 4.

[15] Sarah O'Connor, Fergus Hanson, Emilia Currey, and Tracy Beattie (ASPI), *Cyber-enabled foreign interference in elections and referendums*, 28 October 2020, p. 6.

[16] Dr Jake Wallis and Mr Thomas Uren, ASPI, *Submission 2*, p. 1.

Recommendation 2

1.42 The committee recommends that the Australian Government take a proactive approach to protecting groups that are common targets of foreign interference but are not classified as government institutions.

1.43 The committee notes that there are currently no clear protections for groups that influence Australia's democracy but sit outside of government, such as diaspora groups, research institutions and political parties.

1.44 The committee considered that in the context of high-profile attacks on these groups around the world by authoritarian countries, such as the Pegasus spyware, the government needs to be more proactive in protecting these groups from cyber-enabled foreign interference, such as by offering tools and advice on current threats and how to mitigate them, including in-language resources.

Recommendation 3

1.45 The committee recommends that the Australian Government establish appropriate, transparent, and non-political institutional mechanisms for publicly communicating cyber-enabled foreign interference in our elections and review the processes and protocols for classified briefings for the Opposition during caretaker with respect to cyber-enabled foreign interference.

1.46 The committee refers to the comments of Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its *Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory review of the Security of Critical Infrastructure Act 2018*.

1.47 The PJCIS found that 'foreign interference, disinformation and cyber-attacks are new risks to the free and fair conduct of elections in Australia, the Committee recommends that the caretaker conventions be updated to reflect this new context.'[17]

[17] Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory review of the Security of Critical Infrastructure Act 2018*, September 2021, p. 54.

Recommendation 4

1.48 The committee recommends that the Australian Communications and Media Authority's report into the functioning of the Australian Code of Practice on Disinformation and Misinformation be publicly released as a matter of priority.

1.49 To date, the government has not released the report by the Australian Communications and Media Authority (ACMA) into of the Australian Code of Practice on Disinformation and Misinformation, which covers the adequacy of digital platforms' measures and the broader impacts of misinformation in Australia.[18] While departmental witnesses noted that the report was currently before the relevant minister,[19] there is a clear public interest for the report to be released in order for the efficacy of the currently voluntary code to be assessed by policymakers and the wider research community. At present, ACMA is waiting on the Minister's feedback on the report before further regulatory activity can commence,[20] despite the rapidly approaching Federal Election. ACMA's decision to 'seek to see how things progress over the next couple of months' demonstrates a lack of urgency within government on this matter.[21]

Recommendation 5

1.50 The committee recommends that the Australian Government publicly release the Electoral Integrity Assurance Taskforce's terms of reference.

1.51 The committee also found that departmental arrangements and division of responsibilities around foreign interference through social media were complicated, onerous and lacked transparency. Despite existing since 2018, the Electoral Integrity Assurance Taskforce (EIAT) has not made its terms of reference publicly available.[22] External confusion regarding different agencies' roles within the EIAT is a problem, as is the lack of activity by the EIAT to clearly communicate its approach to the upcoming Federal Election.

---

[18] Australian Communications and Media Authority (ACMA), 'Development of a voluntary code', https://www.acma.gov.au/online-misinformation (accessed 9 August 2021).

[19] Ms Pauline Sullivan, First Assistant Secretary, Online Safety, Media and Platforms Division, Department of Infrastructure, Transport, Regional Development and Communications (DITRDC), *Committee Hansard*, 30 July 2021, p. 38.

[20] Ms Pauline Sullivan, DITRDC, *Committee Hansard*, 30 July 2021, p.38.

[21] Ms Pauline Sullivan, DITRDC, *Committee Hansard*, 30 July 2021, p.38.

[22] Mr Jeff Pope, Deputy Electoral Commissioner, Australian Electoral Commission, *Committee Hansard*, 30 July 2021, p. 25.

1.52 As the EIAT does have a clear role—or, at least, its constituent agencies do—in combatting foreign interference through social media, it is imperative that its terms of reference be released to the public before the next Federal Election. It is the committee's view that public confidence in government bodies, especially those dedicated to electoral integrity, is diminished when a taskforce's terms of reference are hidden. The Australian Government's decision not to publish the terms of reference is unfortunate.

Recommendation 6

1.53 The committee recommends that the Australian Government establish clear requirements and pathways for social media platforms to report suspected foreign interference, including disinformation and coordinated inauthentic behaviour, and other offensive and harmful content, and formalise agency remits, powers and resourcing arrangements accordingly.

1.54 Lastly, the committee was told that existing arrangements for social media platforms to engage with government were inefficient and unclear. At present, should a social media platform identify foreign interference it is optional for them to report it to government.

1.55 While the committee notes that many departments have sought to engage with social media platforms, the lack of a clear reporting process for social media companies is a problem. The committee was concerned by TikTok's acknowledgement that it was unsure who it should inform if it detected foreign interference on its platform.[23] Given the impending Federal Election, it is imperative that the government establish clear policies and procedures for social media platforms to refer potential foreign interference for consideration by the relevant government departments or entities.

Recommendation 7

1.56 The committee recommends that the Election Integrity Assurance Taskforce undertake an audit to assess capability relevant to detecting disinformation prior to the coming election and, further, that the Australian Government consider providing information about relevant capabilities and resourcing to this committee as appropriate to assist in our deliberations.

[23] Mr Lee Hunter, General Manager, TikTok Australia and New Zealand, TikTok Australia, and Mr Thomas, TikTok Australia, *Committee Hansard*, 25 September 2020, p. 12.

Chapter 2
Inquiry details

2.1 On 5 December 2019, the Senate resolved to establish a Select Committee on Foreign Interference through Social Media to inquire into and report on the risk posed to Australia's democracy by foreign interference through social media, with particular reference to:

(a) The use of social media for purposes that undermine Australia's democracy and values, including the spread of misinformation;
(b) responses to mitigate the risk posed to Australia's democracy and values, including by the Australian Government and social media platforms;
(c) international policy responses to cyber-enabled foreign interference and misinformation;
(d) the extent of compliance with Australian laws; and
(e) any related matters.[1]

Conduct of the inquiry

2.2 In accordance with usual practice, the committee advertised the inquiry on its website and wrote to relevant individuals and organisations inviting submissions. The initial date for receipt of submissions was 13 March 2020. On 27 May 2021, the committee announced that submissions would reopen until 31 October 2021. Thus far, the committee has received 43 submissions, which are listed at Appendix 1.

2.3 Despite the substantial disruption caused by the ongoing COVID-19 pandemic, the committee held public hearings in Canberra on:

- 22 June 2020;
- 25 September 2020;
- 11 December 2020; and
- 30 July 2021.

2.4 A list of the organisations and witnesses that attended these public hearings can be found within Appendix 2. The public submissions, additional information received and Hansard transcripts are available on the committee's website:
www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_through_Social_Media

[1] Journals of the Senate, No. 35, 5 December 2019, pp. 1128-1129.

Report structure

2.5 The report contains the following chapters:

- Chapter 1 contains the committee's view and associated recommendations;
- Chapter 2 summarises the context and administrative details of the inquiry, as well as previous domestic reports into the issue of foreign interference through social media in Australia;
- Chapter 3 outlines the mechanisms that are currently being used to combat foreign interference in Australia;
- Chapter 4 explores the key issues raised by submitters and witnesses regarding foreign interference through social media in Australia; and
- Chapter 5 examines the current arrangements the Australian Government has in place to respond to foreign interference through social media.

Scope of the report

2.6 This interim report outlines the nature of foreign interference through social media and the challenges presented to Australia's democracy. In doing so, the report focuses on Facebook,[2] Twitter, Google,[3] TikTok and WeChat as these social media platforms have significant reach globally and within Australia. While foreign interference through social media is a global issue and international examples are referred to in this report, the committee's terms of reference necessitate a focus on the domestic context in Australia. Accordingly, the report considers the issue of foreign interference through social media in the context of the upcoming Federal Election and Australia's ongoing response to the COVID-19 pandemic. The report also considers the arrangements that the Australian Government has established to identify and respond to instances of foreign interference through social media in Australia.

Definitions

2.7 In this report, foreign interference, foreign influence, misinformation and disinformation are utilised to describe distinct phenomena. The Department of Home Affairs observes that these concepts cover a range of activities and, as such, not all influence activities can be considered foreign interference. For example:

- Foreign Interference: Clandestine activities carried out by, or on behalf of, a foreign actor which seek to interfere in decision-making, political discourse or other societal norms. Foreign interference is coercive, covert, deceptive or corrupting and is contrary to Australia's sovereignty, values and national interests.
- Foreign Influence: Overt activities to advocate for particular outcomes or shape consideration of issues important to foreign actors. When

[2] Facebook also owns WhatsApp and Instagram.

[3] Google also owns YouTube.

conducted in an open and transparent manner, these activities can contribute positively to public debate.

- Disinformation: False information designed to deliberately mislead and influence public opinion or obscure the truth for malicious or deceptive purposes. Disinformation can be intended for financial gain (such as clickbait stories), but have an incidental effect on public opinion or debate.
- Misinformation: False information that is spread due to ignorance, by error or mistake with good intentions/without the intent to deceive.[4]

2.8 The committee's terms of reference specifically refer to both foreign interference and misinformation. The impact of foreign influence is not referred to in the committee's terms of reference. Foreign influence is therefore primarily referred to in this report with regard to the Foreign Influence Transparency Scheme, due to the scheme's increased role during election periods and its interactions with the Electoral Integrity Assurance Taskforce.

2.9 Additionally, disinformation—while not directly anticipated by the committee's terms of reference—has many of the same malicious impacts as misinformation and is therefore considered within the report. The 2019 Australian Code of Practice on Disinformation and Misinformation describes disinformation as:

(a) digital content that is verifiably false or misleading or deceptive;
(b) propagated amongst users of digital platforms via inauthentic behaviours; and
(c) the dissemination of which is reasonably likely to cause harm.[5]

Other inquiries and reports

2.10 A range of inquiries and reports have explored the risks posed to Australian democracy by foreign interference through social media. While there are numerous international reports that consider the issues associated with foreign interference through social media and propose solutions in these areas, the reports in this section consider Australia's specific domestic context.

The Australian Strategic Policy Institute

2.11 The Australian Strategic Policy Institute (ASPI) has undertaken a number of relevant reports into foreign interference through social media, as well as the spread of misinformation and disinformation online. A selection of ASPI's reports is outlined below.

---

4 Department of Home Affairs, *Submission 16*, p. 4.

5 Digital Industry Group (DIGI), *Australian Code of Practice on Disinformation and Misinformation*, 22 February 2021, pp. 4-5.

Hacking democracies: Cataloguing cyber-enabled attacks on elections

2.12 On 17 May 2019, ASPI released the report *Hacking democracies: Cataloguing cyber-enabled attacks on elections*. This report sought to catalogue cyber-enabled foreign interference that occurred in elections following Russia's interference in the 2016 United States election, cataloguing the interference into three groups:

- interference targeting voting infrastructure and voter turnout;
- interference in the information environment; and
- longer term efforts to erode public trust in governments, political leadership and public institutions.[6]

2.13 The report found that '[o]f the 97 national elections in free or partly free countries reviewed for this report during the period from 8 November 2016 to 30 April 2019, a fifth (20 countries) showed clear examples of foreign interference, and several countries had multiple examples'.[7] The report recommended that nations:

- recognise the source of foreign interference (namely, Russia and China);
- build up their detection capabilities;
- fund research to measure impact and measure the effectiveness of education campaigns to address public concerns;
- publicly fund the defence of political parties;
- impose costs on adversaries;
- look beyond digital interference in democracies; and
- look beyond other nations as sources of interference, recognising that other actors may be seeking to interfere.[8]

2.14 The report's appendix lists detailed examples of interference in elections that was primarily suspected of being perpetrated by Russia and China, including the Australian 2019 Federal Election. ASPI reported that interference was via the targeting of the Liberal, Labor and National Parties and attempts to access servers located at Parliament House.[9]

Cyber-enabled foreign interference in elections and referendums

2.15 On 28 October 2020, ASPI released its report *Cyber-enabled foreign interference in elections and referendums*, which 'identified 41 elections and seven referendums

---

6 Fergus Hanson, Sarah O'Connor, Mali Walker and Luke Courtois, *Hacking democracies: Cataloguing cyber-enabled attacks on elections*, Australian Strategic Policy Institute, Report No. 16/2019, p. 5.

7 Fergus Hanson, Sarah O'Connor, Mali Walker and Luke Courtois, *Hacking democracies: Cataloguing cyber-enabled attacks on elections*, Australian Strategic Policy Institute, Report No. 16/2019, p. 8.

8 Fergus Hanson, Sarah O'Connor, Mali Walker and Luke Courtois, *Hacking democracies: Cataloguing cyber-enabled attacks on elections*, Australian Strategic Policy Institute, Report No. 16/2019, pp. 17-18.

9 Fergus Hanson, Sarah O'Connor, Mali Walker and Luke Courtois, *Hacking democracies: Cataloguing cyber-enabled attacks on elections*, Australian Strategic Policy Institute, Report No. 16/2019, pp. 26.

between January 2010 and October 2020 where cyber-enabled foreign interference was reported'.[10] The report further noted that '[d]emocratic societies are yet to develop clear thresholds for responding to cyber-enabled interference, particularly when it's combined with other levers of state power or layered with a veil of plausible deniability'.[11]

2.16 The report found that cyber-enabled interference had occurred on six continents, including Australia. It further observed that 33 countries—also including Australia—had experienced cyber-enabled foreign interference in at least one election cycle or referendum.[12]

2.17 The report's view that Australia had previously experienced foreign interference in an election was based on the 2019 Federal Election. The reported stated:

> According to the Sydney Morning Herald, Australian Prime Minister Scott Morrison confirmed on 18 February 2019 that a hacker group had targeted the Liberal, Labor and National parties and accessed the fileservers at Parliament House ahead of the federal election. The Prime Minister noted that the breach, which occurred on 8 February 2019, was the work of a 'sophisticated' but did not make any formal attributions. A number of sources within the Australian Signals Directorate (ASD)—Australia's cyber intelligence agency—confirmed that their investigation had concluded China was responsible.[13]

Joint Standing Committee on Electoral Matters

2.18 The Joint Standing Committee on Electoral Matters (JSCEM) has undertaken a number of inquiries that examine issues related to foreign interference through social media in Australia, most prominently through its reporting on the conduct of the 2019 Federal Election.[14]

2.19 In December 2020, the JSCEM released its final report on the 2019 Federal Election, entitled *Report on the conduct of the 2019 federal election and matters related thereto*, in December 2020. The report noted that '[o]ver the past few

---

[10] Sarah O'Connor, Fergus Hanson, Emilia Currey, and Tracy Beattie, *Cyber-enabled foreign interference in elections and referendums*, Report 41/2020, p. 3.

[11] Sarah O'Connor, Fergus Hanson, Emilia Currey, and Tracy Beattie, *Cyber-enabled foreign interference in elections and referendums*, Report 41/2020, p. 3.

[12] Sarah O'Connor, Fergus Hanson, Emilia Currey, and Tracy Beattie, *Cyber-enabled foreign interference in elections and referendums*, Report 41/2020, p. 9.

[13] Sarah O'Connor, Fergus Hanson, Emilia Currey, and Tracy Beattie, *Cyber-enabled foreign interference in elections and referendums*, Report 41/2020, p. 25.

[14] The committee has also released a report into the 2016 election: see Joint Standing Committee on Electoral Matters (JSCEM), *Report on the conduct of the 2016 federal election and matters related thereto*, November 2018.

years there has been a significant rise in the proliferation of disinformation and misinformation, particularly on social media and search platforms'.[15]

2.20 Ultimately, the committee reported that it had not found substantive foreign interference via social media during the 2019 Federal Election:

> The JSCEM also found limited evidence of social media manipulation within Australia, including minimal use of bots. However, given the significant rise in organised social media manipulation campaigns, we must remain vigilant.[16]

2.21 The report made a number of pertinent recommendations that are pertinent to this inquiry, including:

> Recommendation 14: The Committee recommends that the current work of the Australian Competition and Consumer Commission and the Australian Communications and Media Authority to adapt regulation so it can keep pace with technological change, clearly addresses electoral and political advertising. It also recommends these agencies form a working group with the Australian Electoral Commission and other key stakeholders to ensure this important area is addressed as a priority.[17]
>
> Recommendation 15: The Committee recommends that the Electoral Integrity Assurance Taskforce be engaged permanently to prevent and combat cyber manipulation and electoral/foreign interference in Australia's democratic process and to provide post-election findings regarding any pertinent incidents to the Joint Standing Committee on Electoral Matters, including through in camera and open briefing.[18]

2.22 At the time of writing, the Australian Government has not responded to this report.

Australian Competition and Consumer Commission

2.23 The Australian Competition and Consumer Commission (ACCC) has undertaken two inquiries into digital platforms, which are described below.

Digital platforms inquiry

2.24 On 26 July 2019, the ACCC released its final report on its digital platforms inquiry. The inquiry examined the impact of digital platforms on consumers, businesses using platforms to advertise to and reach customers, and news media businesses that also use the platforms to disseminate their content.

---

[15] JSCEM, *Report on the conduct of the 2019 federal election and matters related thereto*, December 2020, p. 105.

[16] JSCEM, *Report on the conduct of the 2019 federal election and matters related thereto*, December 2020, p. 122.

[17] JSCEM, *Report on the conduct of the 2019 federal election and matters related thereto*, December 2020, p. xviii.

[18] JSCEM, *Report on the conduct of the 2019 federal election and matters related thereto*, December 2020, p. xviii.

2.25 The report found that the ubiquity of the Google and Facebook platforms has placed them in a privileged position. Moreover, the report found that the opaque operations of digital platforms and their presence in interrelated markets means that it is difficult to determine precisely what standard of behaviour these digital platforms are meeting.[19]

2.26 The ACCC noted that the collection of user data is central to the business models of most advertiser-funded platforms. User data enables digital platforms to offer highly targeted or personalised advertising opportunities to advertisers, enabling platforms to provide highly tailored products to advertisers.[20]

2.27 The ACCC observed that while Australian consumers benefit from the many 'free' services offered by digital platforms and most users have at least some understanding that certain types of user data and personal information are collected in return for their use of a service, few consumers are fully informed of, fully understand or effectively control the scope of data collected and the bargain they are entering into with digital platforms when they sign up for or use their services.[21]

2.28 The ACCC expressed concern that the existing regulatory frameworks for the collection and use of data have not held up well to the challenges of digitalisation and the practical reality of targeted advertising that rely on the monetisation of consumer data and attention.[22] These concerns were not limited to digital platforms, with an increasing number of businesses across the economy collecting and monetising consumer data.

2.29 The ACCC recommended that the *Privacy Act 1988* (the Privacy Act) be amended to ensure consumers are adequately informed, empowered and protected as to how their data is being used and collected. The ACCC also suggested that now is the time to consider the current and likely future issues associated with digital platforms and their business models and to put in place frameworks that enable adverse consequences to be addressed and that reduce the likelihood of new issues arising.[23]

---

[19] Australian Competition and Consumer Commission (ACCC), *Digital platforms inquiry: final report*, June 2019, p. 1 and p. 7.

[20] ACCC, *Digital platforms inquiry: final report*, June 2019, p. 2.

[21] ACCC, *Digital platforms inquiry: final report*, June 2019, p. 2.

[22] ACCC, *Digital platforms inquiry: final report*, June 2019, p. 3.

[23] ACCC, *Digital platforms inquiry: final report*, June 2019, p. 3.

Government response and ongoing activities

2.30 On 12 December 2019, the Australian Government released its response to the digital platforms inquiry's final report. The Australian Government committed to:

- establishing a special unit in the ACCC to monitor and report on the state of competition and consumer protection in digital platform markets, take enforcement action as necessary, and undertake inquiries as directed by the Treasurer, starting with the supply of online advertising and ad-tech services;
- addressing bargaining power concerns between digital platforms and media businesses by tasking the ACCC to facilitate the development of a voluntary code of conduct;
- commencing a staged process to reform media regulation towards an end state of a platform-neutral regulatory framework covering both online and offline delivery of media content to Australian consumers; and
- ensuring privacy settings empower consumers, protect their data and best serve the Australian economy by building on our commitment to increase penalties and introduce a binding online privacy code announced in the 2019-20 Budget, through further strengthening of Privacy Act protections, subject to consultation and design of specific measures as well as conducting a review of the Privacy Act.[24]

2.31 The Attorney-General's Department has commenced its review of the Privacy Act. On 30 October 2020, the Department released an issues paper that outlined current privacy laws and sought feedback on potential issues relevant to reform, which included the terms of reference for the review. The review will cover:

- the scope and application of the Privacy Act;
- whether the Privacy Act effectively protects personal information and provides a practical and proportionate framework for promoting good privacy practices;
- whether individuals should have direct rights of action to enforce privacy obligations under the Privacy Act;
- whether a statutory tort for serious invasions of privacy should be introduced into Australian law;
- the impact of the notifiable data breach scheme and its effectiveness in meeting its objectives;
- the effectiveness of enforcement powers and mechanisms under the Privacy Act and how they interact with other Commonwealth regulatory frameworks; and

[24] Treasury, 'Government Response and Implementation Roadmap for the Digital Platforms Inquiry', *Government Response*, 12 December 2019.

- the desirability and feasibility of an independent certification scheme to monitor and demonstrate compliance with Australian privacy laws.[25]

2.32 On 30 July 2021, Ms Julia Galluccio, Assistant Secretary, Information Law Branch, Attorney-General's Department, updated the committee on the progress of the report, stating that the Department had received 200 submissions in response to the issues paper and was now 'in the process of finalising a discussion paper which will, again, be released for public consultation'.[26] Ms Galluccio stated that, following this discussion paper, the Department would begin its final report.[27]

2.33 Additionally, on 25 October 2021 the Attorney-General's Department released an exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, which seeks to strengthen the Privacy Act through 'enabl[ing] the introduction of a binding online privacy code for social media and certain other online platforms, and increases penalties and enforcement measures'.[28]

2.34 Another element of the Federal Government's response to the Digital platforms inquiry was that the major digital platforms would put in place a voluntary code of conduct for disinformation and news quality.[29] The Australian Communications and Media Authority (ACMA) had been tasked to report to government on the adequacy of the platforms' measures and the broader impacts of disinformation by June 2021.[30] This process entailed ACMA consulting with digital platforms, government and other relevant stakeholders to develop principles and minimum expectations for a voluntary code of conduct.[31] This report is yet to be released.

2.35 On 26 June 2020, ACMA released a position paper outlining its expectations for a voluntary code or codes of practice on misinformation and news quality to be developed by digital platforms.[32] A final code of practice for social media platforms was published in February 2021, entitled *The Australian code of*

---

25 Attorney-General's Department, *Privacy Act review: issues paper*, 30 October 2020, p. 2.

26 Ms Julia Galluccio, Assistant Secretary, Information Law Branch, Attorney-General's Department, *Committee Hansard*, 30 July 2021, p. 36.

27 Ms Julia Galluccio, Attorney-General's Department, *Committee Hansard*, 30 July 2021, p. 36.

28 Attorney-General's Department, 'Online Privacy Bill Exposure Draft', https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/ (accessed 7 December 2021).

29 ACMA, *Submission 15*, p. 1.

30 ACMA, *Submission 15*, p. 2.

31 ACMA, *Submission 15*, p. 2.

32 ACMA, 'ACMA releases guidance to digital platforms on voluntary misinformation and news quality code', *Media release*, 26 June 2020.

practice on disinformation and misinformation. The code has been adopted by Twitter, Google, Facebook, Microsoft, Redbubble, TikTok, Adobe and Apple.[33]

Digital platform services inquiry 2020-2025

2.36 Following the digital platforms inquiry, on 10 February 2020 the Australian Government directed the ACCC to conduct an inquiry into markets for the supply of digital platform services, which has been entitled *Digital platform services inquiry 2020-2025*. Matters to be undertaken by the inquiry include:

- the intensity of competition in markets for the supply of digital platform services, with particular regard to the concentration of power, the behaviour of suppliers, mergers and acquisitions, barriers to entry or expansion and changes in the range of services offered by suppliers of digital platform services;
- practices of suppliers in digital platform services markets which may result in consumer harm;
- market trends that may affect the nature and characteristics of digital platform services; and
- developments in markets for the supply of digital platform services outside Australia.[34]

2.37 Thus far, the ACCC has released two interim reports. The September 2020 interim report, which was released on 23 October 2020, examines online private messaging services in Australia, updates the ACCC's previous analysis in relation to search and social media platforms, and identifies competition and consumer issues common across these platforms.[35]

2.38 The March 2021 interim report, which was released on 28 April 2021, provides in-depth consideration of competition and consumer issues associated with the distribution of mobile apps to users of smartphones and other mobile devices. It specifically focuses on the two key app marketplaces used in Australia, the Apple App Store and the Google Play Store.[36]

News and Media Research Centre

2.39 The University of Canberra's News and Media Research Centre (NMRC) has released two digital news reports, the *Digital news report: Australia 2020* (16 June 2020) and *Digital news report: Australia 2021* (23 July 2021). These reports

---

[33] DIGI, 'Australian Code of Practice on Disinformation and Misinformation', https://digi.org.au/disinformation-code/ (accessed 9 August 2021).

[34] ACCC, *Digital platform services inquiry 2020-2025: September 2020 interim report*, September 2020, p. 9.

[35] ACCC, *Digital platform services inquiry 2020-2025: September 2020 interim report*, September 2020, p. 9.

[36] ACCC, *Digital platform services inquiry 2020-2025: March 2021 interim report,* April 2021, p. 3.

are part of a long running international survey coordinated by the Reuters Institute for the Study of Journalism, an international research centre based at the University of Oxford. The Digital news reports deliver comparative data on media usage in 40 countries and across six continents.[37]

Digital news report: Australia 2020

2.40 *Digital news report: Australia 2020* examined the domestic media context in Australia and particularly how Australians consume their news. Some of the report's key findings included that:

- Australian news consumers are accessing news more frequently, but their interest in news is declining;
- half of Generation Z,[38] and 30 per cent of people aged 74 and over, use Facebook for news;
- trust in news fell to 38 per cent in January and February of 2020, but trust in news about COVID-19 during the pandemic was much higher (53 per cent);
- more than half (54 per cent) of news consumers say they prefer impartial news, but 19 per cent want news that confirms their worldview; and
- more than half (58 per cent) believe tech platforms should block false political ads and 24 per cent say they should not.[39]

2.41 The report particularly noted that there is rising community concern about political advertising on social media:

> There is more concern about political advertising on social media than on TV. Half of Australians think political ads on TV are OK, but don't feel comfortable about social media. When it comes to false ads, the majority think the tech platforms, Google and Facebook, should block them. This is particularly true of leftwing consumers. The success of the Coalition advertising and the failure of the Labour campaign during the 2019 federal election might help explain some of this difference. However, about one-quarter of Australians do not think that it is the responsibility of tech companies to decide what is true or false. In an age where political mendacity appears to be rising, these are important discussions for the public, news media and legislators to have.[40]

---

[37] Sora Park, Caroline Fisher, Jee Young-Lee, Kieran McGuinness, Yoonmo Sang, Mathieu O'Neil, Michael Jensen, Kerry McCallum, and Glen Fuller, *Digital news report: Australia 2020*, July 2020, p. 4.

[38] Primarily includes people born in mid-to-late 1990s to those born in the early 2010s.

[39] Sora Park, Caroline Fisher, Jee Young-Lee, Kieran McGuinness, Yoonmo Sang, Mathieu O'Neil, Michael Jensen, Kerry McCallum, and Glen Fuller, *Digital news report: Australia 2020*, July 2020, pp. 12-13.

[40] Sora Park, Caroline Fisher, Jee Young-Lee, Kieran McGuinness, Yoonmo Sang, Mathieu O'Neil, Michael Jensen, Kerry McCallum, and Glen Fuller, *Digital news report: Australia 2020*, July 2020, p. 104.

Digital news report: Australia 2021

2.42 *Digital news report: Australia 2021*, like its predecessor, examined news consumption behaviour in Australian. The report tracks the impact of the COVID-19 pandemic on news consumers during the 2020-21 period.[41] The report's key findings were that:

- trust in news increased globally over the past 12 months: in Australia, trust in news has risen (+5) to 43 per cent, close to the global average (44 per cent);
- Australians' interest in news dropped during the pandemic in line with other countries, and interest in the news has been consistently declining among Australian audiences;
- general concern about false and misleading information online in Australia is high (64 per cent), and much higher than the global average (56 per cent);
- women, younger generations and those with low income are less likely to see themselves or their views as being fairly or sufficiently reflected in the news; and
- the majority of Australians (66 per cent) are either unaware that commercial news organisations are less profitable than they were 10 years ago, or they don't know about the current financial state of the news media.[42]

Australian perspectives on misinformation

2.43 The November 2020 report *Australian perspectives on misinformation* arises from the results of two of the NMRC's previous reports, *Digital news report: Australia 2020* and *COVID-19: Australian news and misinformation*. The report addresses the targeting of Australian society by foreign interference operations, specifically by its examination of a Russian-based Twitter campaign that occurred in the lead-up to the 2016 Federal Election.[43]

---

41 Sora Park, Caroline Fisher, Kieran McGuinness, Jee Young Lee, and, Kerry McCallum, *Digital news report: Australia 2021*, June 2021, p. 8.

42 Sora Park, Caroline Fisher, Kieran McGuinness, Jee Young Lee, and, Kerry McCallum, *Digital news report: Australia 2021*, June 2021, pp. 9-11.

43 Dr Mathieu O'Neil and Dr Michael Jensen, *Australian perspectives on misinformation*, November 2020, p. 9.

Chapter 3
Mechanisms

3.1 The spread of foreign interference on social media uses significantly different mechanisms to other forms of cyber-attacks. Foreign interference can occur via direct means, such as attempts at brute-force hacking to gain access to Australian systems, attempts to gain access through deceiving users, and using distributed denial-of-service attacks. These methodologies are used to gain access to Australian information that may be of use or interest abroad and to otherwise disrupt Australian services.

3.2 Foreign interference can also occur via indirect means, such as through commonly used and trusted social media platforms. This form of foreign interference and disruption by social media is much harder for end users to detect and includes coordinated inauthentic behaviour (CIB), algorithmic curation, microtargeting, the use of bots, human-driven interference and automated moderation. This chapter describes how these mechanisms operate and their potential impact.

Coordinated inauthentic behaviour

3.3 The term 'coordinated inauthentic behaviour' (CIB) is a classification used by many social media companies to define undesirable behaviour. For example, Facebook describes CIB as:

> …coordinated efforts to manipulate public debate for a strategic goal where fake accounts are central to the operation.[1]

3.4 Facebook further notes that CIB does not necessarily need to come from a government actor:

> There are two tiers of these activities that we work to stop:
>
> 1) coordinated inauthentic behavior in the context of domestic, non-government campaigns and
>
> 2) coordinated inauthentic behavior on behalf of a foreign or government actor.[2]

3.5 A key element of CIB is that the source of the coordinated effort seeks to hide their identity. Facebook notes that the term CIB also includes 'any coordinated effort to mislead the public about who's behind an operation through the use of fake accounts and deceptive behaviour'.[3] Similarly, Mr Lee Hunter, General

---

1 Facebook, *August 2020 Coordinated Inauthentic Behavior Report*, 1 September 2020, p. 2.

2 Facebook, *August 2020 Coordinated Inauthentic Behavior Report*, 1 September 2020, p. 2.

3 Mr Nathaniel Gleicher, Global Head of Security Policy, Facebook, *Committee Hansard*, 30 July 2021, p. 3.

Manager, TikTok Australia and New Zealand, TikTok Australia, described CIB as individuals and groups who 'disguise their purpose and their identity to influence matters of importance to Australia'.[4]

3.6 This report utilises the term CIB to refer to activities that include coordinated foreign interference through social media, as well as other organised attempts to spread disinformation.

Algorithmic curation

3.7 The use of algorithms on social media platforms is ubiquitous. An algorithm is a program that runs in the background on social media platforms, analysing users' behaviour and tailoring users' social media feed. Algorithms select content based on factors such as a user's past online activity, social connections, and their location.[5] Social media platforms use algorithms to build profiles, which are not visible to users, that collate available information about users for corporate use, including selling targeted advertising.

3.8 While algorithms are primarily used to maintain user interest, they tend to default to highly attention-grabbing content. Responsible Technology Australia described how algorithms can be used to promote extreme and inflammatory material:

> As the primary aim of these platforms is to maximise user time spent on them (to increase their advertising revenue potential), the algorithms are incentivised to serve material that is calculated to engage users more. This content tends to be more extremist or sensationalist or untrue - as it has been shown to be more captivating. This opens the door for foreign agents to seed inflammatory and sensational content that users engage with out of outrage or support, and is then amplified by the algorithms which see all engagement as warranting amplification - regardless of the nature of the content.[6]

3.9 Additionally, algorithms used on social media platforms may encourage engagement with inflammatory content. As users' feeds are tailored towards the individual's interests and political beliefs, this can result in an 'echo chamber' effect and progressive engagement with more extreme content.[7]

3.10 Algorithms used by social media platforms to target material (including advertisements) are not generally publicly available, nor are the 'nudges' delivered by these algorithms transparent to users. In reference to Facebook, Allens Hub for Technology, Law and Innovation; the Datafication and

---

[4] Mr Lee Hunter, General Manager, TikTok Australia and New Zealand, TikTok Australia, *Committee Hansard*, 25 September 2020, p. 11.

[5] Responsible Technology Australia, *Submission 17*, pp. 1-2.

[6] Responsible Technology Australia, *Submission 17*, p. 2.

[7] The Department of Home Affairs, *Submission 16*, p. 4.

Automation of Human Life; and the Society on Social Implications of Technology (Allens Hub et al) submitted that 'each user knows what they see on Facebook, but no individual is privileged to see the underlying algorithm driving what others are seeing'.[8]

Microtargeting

3.11 In extreme cases, algorithmic curation of social media feeds can result in users inhabiting an online environment that is not reflective of real-world conditions. While the use of algorithms described above could be described the 'normal' state of being on social media platforms, microtargeting is the weaponisation of the social media environment in order to further the goals of various actors—corporate, international and even malicious. Responsible Technology Australia described the practice as targeted advertising:

> The unfettered approach to data collection has amassed history's largest data sets, allowing advertisers to push beyond normal constraints to deliver direct and granular targeting of consumers. This microtargeting often uses key emotional trigger points and personal characteristics to drive outcomes, which malicious actors can easily exploit to sow distrust, fear and polarisation.[9]

3.12 Similarly, the Department of Home Affairs observed that:

> …social media can selectively deliver tailored messaging through the microtargeting of audiences identified by 'big data' analytics'. This is generally the result of previous behaviours displayed by the user, or based upon the network of people or groups they follow. The delivery of different messages to different audiences is very much a feature of the 'echo chamber' effect which can drive political and social polarisation on social media. This can occur when users are continually receiving self-reinforcing communications based upon their previous online behaviours or social networks, at the expense of different views or information.[10]

3.13 The Joint Select Committee on Electoral Matters' *Report on the Conduct of the 2016 Federal Election* described the phenomenon as 'dark advertising', which 'allows groups and companies to target specific individuals or groups (micro-targeting), with the goal of shifting their opinions. It is different from normal advertising because it will be seen by only the intended recipient.'[11]

3.14 The Australia Institute submitted that the lack of transparency associated with microtargeting was particularly problematic, as it 'limits scrutiny and

---

[8] Allens Hub for Technology, Law and Innovation; the Datafication and Automation of Human Life; and the Society on Social Implications of Technology (Allens Hub et al), *Submission 19*, p. 2.

[9] Responsible Technology Australia, *Submission 17*, p. 2.

[10] Department of Home Affairs, *Submission 16*, p. 4. See also Allens Hub et al, *Submission 19*, p. 2.

[11] Joint Standing Committee on Electoral Matters (JSCEM), *Report on the conduct of the 2016 federal election and matters related thereto*, November 2018, p. 176. See also Law Council, *Submission 18*, p. 11.

accountability since most of the public never see the message'.[12] The Australia Institute further outlined that, by its very nature, microtargeting could focus on highly specific groups:

> Micro-targeting gives the ability to target very specific combinations of demographics, psychographics, user preferences, consumption habits and more to profile voters and spread targeted misinformation.[13]

3.15 Responsible Technology Australia likewise stated that the potential for the microtargeting of individuals in this fashion is completely unprecedented, leaving Australians 'extremely vulnerable to many different forms of manipulation by foreign and malicious actors who wish to threaten the Australian democratic process, exploit our declining trust in our public institutions and generally divide Australian society at large.'[14]

3.16 Facebook's products enable a high degree of microtargeting. The most notable example of this practice was the activities of Cambridge Analytica, where 87 million users' private data was harvested and used to better target political advertisements in the 2016 United States presidential election and the 2016 Brexit campaign. Facebook was eventually fined in the United Kingdom for its conduct.[15] The Office of the Australian Information Commissioner (OAIC) launched Federal Court action against Facebook, considering its collection of information to be in breach of the *Privacy Act 1988*. The OAIC stated in a media release that:

> We claim these actions left the personal data of around 311,127 Australian Facebook users exposed to be sold and used for purposes including political profiling, well outside users' expectations.[16]

3.17 While Facebook denied that it was undertaking business in Australia, and thus was not in breach of Australia's privacy laws, on 14 September 2020 the Federal Court rejected this assessment and stated that the OAIC had established a prima facie case that Facebook was carrying on business in Australia.[17] As at the time of writing, Facebook is appealing this decision.

---

12 Australia Institute, *Submission 31*, p. 17.

13 Australia Institute, *Submission 31.1*, p. 2.

14 Responsible Technology Australia, *Submission 17*, p. 3. The Law Council of Australia also raised the issue of micro-targeting: see Law Council of Australia, *Submission 18*, pp. 11-12 and pp. 37-39.

15 See JSCEM, *Report on the conduct of the 2016 federal election and matters related thereto*, November 2018, pp. 174-175.

16 Office of the Australian Information Commissioner, 'Commissioner launches Federal Court action against Facebook', *Media Release*, 9 March 2020.

17 Office of the Australian Information Commissioner, 'Commissioner welcomes ruling on Facebook application', *Media Release*, 14 September 2020.

Bots

3.18 A common method of foreign interference and/or influence on social media is the use of 'bots', which are artificial social media accounts that mimic the behaviour of real users. The United Kingdom's House of Commons' Digital, Culture, Media and Sport Committee's *Disinformation and 'Fake News': Interim Report* described bots as:

> …algorithmically-driven computer programmes designed to carry out specific tasks online, such as analysing and scraping data. Some are created for political purposes, such as automatically posting content, increasing follower numbers, supporting political campaigns, or spreading misinformation and disinformation.[18]

3.19 Bots can be difficult to identify and remove and are sometimes sufficiently 'intelligent' to interact with accounts operated by real people. These bots can be used to spread rumours, promote individuals and otherwise rapidly spread disinformation online, including undertaking widespread CIB.

3.20 In their submission, the Allens Hub et al described some of the activities that bots are used for online:

> Bots may constantly share content from particular accounts, regularly post particular content, or respond to content that meets particular criteria in standard ways. In automating sharing and tagging content, bots are able to amplify the number of people reading a particular post because the number of accounts commenting or sharing content is often relevant in determining visibility of content in individual feeds. Therefore, bots make it seem as if particular viewpoints have more support in a community than what is in fact the case.[19]

Human labour

3.21 While foreign interference through social media can be attempted by using new technologies, such as bots or microtargeting, human labour is still used to artificially influence discourse on social media and in attempts at CIB.

3.22 Ms Katherine Mansted noted that, at a base level, large cohorts of bots are still driven by a human that has directed them to undertake an activity:

> What we've seen so far in the space of disinformation online is very much driven by humans still, even when we talk about the use of bots. Generally, bots are used to amplify messages. Those nefarious messages are still generated and curated by humans, often working under quite obscene conditions in the troll factories of the Kremlin, in the 50 cent army in China and in other places.[20]

---

[18] House of Commons, Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim report*, 29 July 2018, p. 19.

[19] Allens Hub et al, *Submission 19*, p. 2.

[20] Ms Katherine Mansted, *Committee Hansard*, 22 June 2020, p. 20.

3.23 People are paid to undertake labour online that includes many of the same activities that are undertaken by bots. Mr Alex Stamos, Director, Stanford Internet Observatory, likewise noted that a common assumption is that the spread of disinformation online is solely spread by bots, when human workers are still widely utilised:

> One of the core misunderstandings here is how people use the term 'bots' too much: 'That's all automated; it's all bots; it's all automatic.' The vast majority of this activity is being done by humans. We should not underestimate how cheap it is in some of these countries to build up very large armies of people to spend all day doing this work.[21]

3.24 Such behaviour, whether undertaken by humans or bots, tends to be banned by most social media platforms. Ms evelyn douek noted that 'all of the platforms now have a rule that you can't have 100 people in St Petersburg pretend to be 10,000 Americans or 10,000 Australians'.[22]

3.25 Additionally, Mr Stamos noted that while there were actors online who were being paid to spread the messages of foreign governments on social media, the vast majority of politically engaged accounts in the Australian social media context were being operated by domestic individuals:

> The number of Australians who care about Australian politics vastly outstrips all of the people Australia's adversaries can hire to sit and read and write English. The number of people who are self-motivated or who are part of political parties or political campaigns who want to do this work is much greater than the number of foreign adversaries, so the domestic problem is something we have to really worry about.[23]

Automated content moderation

3.26 Regarding the removal of misinformation and disinformation from their platform, as well as CIB, most social media platforms utilise a mixture of automated technology and human investigators. Facebook uses both automated technology and human investigators,[24] and it described the benefits of this technology to the committee:

> Our detection technology helps us block millions of attempts to create fake accounts every day, and we detect millions more often within minutes after creation. We removed 1.5 billion fake accounts between April and June 2020, the majority of these accounts were caught within minutes of registration. Of these, 99.6 per cent of these accounts were detected proactively via artificial intelligence, before they were reported to us.[25]

---

21 Mr Alex Stamos, Director, Stanford Internet Observatory, *Committee Hansard*, 22 June 2020, pp. 7-8.

22 Ms evelyn douek, *Committee Hansard*, 22 June 2020, p. 6.

23 Mr Alex Stamos, Stanford Internet Observatory, *Committee Hansard*, 22 June 2020, p. 7.

24 Facebook, *Submission 27*, p. 8.

25 Facebook, *Submission 27*, p. 8.

3.27 Facebook also has more than 35,000 people who 'work with technology to apply their own experience and knowledge to detect and assess possible networks of CIB'.[26] However, Facebook noted that while such automated systems were important, they were not a 'silver bullet':

> These systems work very well at scale, but we know that, as with any automated system, sophisticated actors can get past them if they're determined and well resourced. That's why we complement technology with teams of threat intelligence analysts that hunt for and disrupt cybercriminals, [advanced persistent threats] and influence operators.[27]

3.28 Google likewise noted that on its platform '95 per cent of misinformation videos are flagged by our automated systems' and that it also utilises human analysis to remove CIB.[28]

3.29 Twitter utilises automated content moderation, with 65 per cent of the detected content being reviewed by its employees.[29] Ms Kara Hinesley, Director of Public Policy, Australia and New Zealand, Twitter, described how the two function together:

> Globally, between July and December 2020, our internal proactive tools challenged over 143 million accounts for engaging in suspected spamming behaviour, including those engaged in suspected platform manipulation. From the outset of any election, we also establish a dedicated internal cross-functional team to lead our election integrity work.[30]

3.30 TikTok currently uses a mixture of technology and human moderation for analysing the videos posted to its platform:

> We have technology which looks at videos and applies a view through machine learning to try and understand the content therein and to try and either restrict it immediately, on the basis that it goes against our community guidelines, or pass it along to a human moderator so that they can look at that content and decide whether it's fit for being on the TikTok platform.[31]

3.31 TikTok also noted attempts to circumvent automated content moderation technology were occurring, which posed difficulties.[32]

---

[26] Facebook, *Submission 27*, p. 8.

[27] Mr Nathaniel Gleicher, Facebook, *Committee Hansard*, 30 July 2021, p. 3.

[28] Mrs Lucinda Longcroft, Director, Government Affairs and Public Policy, Australia and New Zealand, Google Australia, *Committee Hansard*, 30 July 2021, p. 12.

[29] Ms Kara Hinesley, Director of Public Policy, Australia and New Zealand, Twitter, *Committee Hansard*, 30 July 2021, p. 47.

[30] Ms Kara Hinesley, Twitter, *Committee Hansard*, 30 July 2021, p. 47.

[31] Mr Lee Hunter, TikTok Australia and New Zealand, *Committee Hansard*, 25 September 2020, p. 18.

[32] In this particular case, the beginning of a video with extreme content was spliced with innocuous content in order to avoid the automatic moderation system: see Mr Lee Hunter, TikTok Australia and New Zealand, *Committee Hansard*, 25 September 2020, p. 19.

3.32 Ms evelyn douek submitted that, during the COVID-19 pandemic, the social media platforms' workers were, in some cases, restricted from attending their workplaces. Subsequent to this, Ms douek noted that 'platforms had to enforce [their] policies and their other rules relying on artificial intelligence tools more than normal'.[33] Ms douek described how this particular environment revealed systemic problems with automated content moderation:

> After usually promoting these tools as a panacea for content-moderation issues, in a moment of unusual candour the platforms all acknowledged that this greater reliance on AI would result in more mistakes. This came as no surprise to researchers in this space, who for years have been warning about the risks of error, bias and lack of contextual analysis associated with using these tools.[34]

[33] Ms evelyn douek, *Committee Hansard*, 22 June 2020, p. 2.

[34] Ms evelyn douek, *Committee Hansard*, 22 June 2020, p. 2.

Chapter 4
Key issues

4.1 This chapter outlines how the scale, speed and relatively low cost of social media campaigns contribute to the spread of coordinated inauthentic behaviour (CIB), misinformation and disinformation online, as well as the motivations of the actors who choose to undertake these activities. In addition, the chapter considers how social media companies' business models may contribute to negative social outcomes, including the undermining of Australia's democratic institutions, a rise in social polarisation, and increasing COVID-19 misinformation and disinformation.

Motivations

4.2 Misinformation, disinformation and CIB can spread across social media rapidly, and is a relatively inexpensive tool for individuals and state actors. The Department of Home Affairs submitted that:

> Social media is an ideal platform for propaganda. The platforms are largely globalised and in many cases fall outside the regulatory arrangements for traditional media, broadcasting, and communications and carriage service providers. Additionally, the platforms are accessed by billions of people and are intrusive of privacy in ways that support tailored messaging. In the worst cases, the platforms can be used to promulgate 'fake news' and provocatively partisan content, undermine social cohesion and sow discontent (or at least confusion).[1]

4.3 The News and Media Research Centre noted that the problem was exacerbated by three factors, which made CIB a preferred course of action for those seeking to undertake foreign interference via social media:

- digital networks play a central role in political communication;
- the speed of social media renders information attacks hard to counter; and
- digital influence operations have low implementation costs.[2]

4.4 Dr Jake Wallis, Senior Analyst, International Cyber Policy Centre, the Australian Strategic Policy Institute (ASPI), noted that malign actors abroad have found foreign interference through social media to be a powerful and cost-effective tool:

> Access to accurate and unbiased information is a precondition for effective decision-making, yet malign actors are engaged in organised and concerted efforts to manipulate the information environment to achieve their strategic goals. Authoritarian states have identified influence

[1] Department of Home Affairs, *Submission 16*, p. 4.

[2] News and Media Research Centre, *Submission 8*, p. pp. 2-3.

> operations as a cheap yet effective mechanism for influencing and weakening liberal democratic societies and regional alliances.[3]

4.5 Individuals who engage in spreading misinformation and disinformation online can have varied motivations. Mr Robert Size discussed some of these motivations:

> …the common conception of fake news is that its publication is ideologically motivated—that those on the fringes of the political spectrum spread false information to push their own agendas, or that foreign powers spread false information to destabilise social and political systems. Undoubtedly, there is truth to this common conception. But the reality of the situation is more complicated. People have all kinds of reasons to spread false information online. Some do it in pursuit of a personal or political agenda. Some do it to shock or insult or enrage. Some do it in the belief (sometimes justified, sometimes not) that readers will interpret their content to be satire. But many, in particular those who publish real fake news (i.e. websites that masquerade as news websites), do it to turn a profit via advertising.[4]

4.6 Dr Jake Wallis and Mr Thomas Uren, ASPI, observed the financial motivations behind the activities that occur online and particularly on social media platforms:

> Social media companies are not exchanging quality content for audience and rely instead on user generated content to attract audiences for advertising. This has resulted in changed incentives for 'news' and content producers. Online, financial incentives are linked to audience size—views, eyeballs, or clicks—and sensationalist and provocative content gathers more engagement, so content producers are de facto encouraged to produce sensationalist content, not necessarily high-quality journalism or even journalism of any sort.
>
> The governance models and ethics that previously applied to traditional journalism have been replaced on social media; absent restraining forces, the default profit- maximising behaviour for social media platforms is to allow sensationalist, provocative content. In this social media ecosystem foreign interference and malign actors can flourish.[5]

4.7 Additionally, financial incentives are not necessarily discrete from political motivations. Dr Jake Wallis, ASPI, further noted that between political ideology and financial motives:

> Often, when we look at fringe politically motivated actors and their behaviours on the internet, they will display similar behaviours. There is often an overlap of political ideology and financial motivation because the finances sustain the operation. These kinds of actors can build little

---

[3] Dr Jake Wallis, Senior Analyst, International Cyber Policy Centre, Australian Strategic Policy Institute (ASPI), *Committee Hansard*, 22 June 2020, p. 10. See also Dr Carlo Kopp, *Committee Hansard*, 22 June 2020, p. 35.

[4] Mr Robert Size, *Submission 3*, p. 2.

[5] Dr Jake Wallis and Mr Thomas Uren, ASPI, *Submission 2*, p. 5.

> ecosystems of websites and podcasts and then run social media channels that steer audiences off into these little ecosystems—that can be quite self-sustaining financially. So there often is an overlap.[6]

4.8 However, it is also clear that foreign state actors are undertaking CIB attempts online. The Department of Home Affairs noted that it regularly observes 'campaigns unfolding on social media that involve disinformation', which it subsequently refers to the host platform for removal.[7] Some of these disinformation cases have been linked to foreign state actors:

> In 2017, following a terrorist attack in Brighton, Melbourne, the Department identified Tweets associated with accounts that have since been publicly attributed by Twitter to a foreign government entity.
>
> In another Australian example from 2017, accounts linked to the same foreign government entity were involved in discussions related to a plot to bomb an Etihad airlines flight departing Sydney International Airport. One account used the disrupted plot to promote and amplify the hashtags "#MuslimBan" and "#StopImportingIslam". In this instance, hostile foreign state actors used social media to interfere in Australia's public discourse and attempt to undermine social cohesion.[8]

Scale

4.9 Social media platforms provided evidence to the committee that outlined their attempts to reduce misinformation, disinformation and CIB on their platforms. Given that social media platforms are the only party with a full view of what is occurring on their platforms, this evidence is critical to understanding the scope of foreign interference and CIB attempts that are carried out on social media, as well as the spread of misinformation and disinformation.

4.10 Google, which also owns the video sharing platform YouTube, described some of the issues it faces:

> Government-backed or State-sponsored groups who attempt to gain access to our user's accounts have varying goals in carrying out operations targeting Google's products: Some are looking to collect intelligence or steal intellectual property; others are targeting dissidents or activists, or attempting to engage in coordinated influence operations and disinformation campaigns. Our products are designed with robust built-in security features, like Gmail protections against phishing and Safe Browsing in Chrome, but we still dedicate significant resources to developing new tools and technology to help identify, track and stop this kind of activity as it evolves.[9]

---

6 Dr Jake Wallis, ASPI, *Committee Hansard*, 22 June 2020, p. 13. See also Ms Katherine Mansted, *Committee Hansard*, 22 June 2020, p. 18.

7 Department of Home Affairs, *Submission 16,* p. 7.

8 Department of Home Affairs, *Submission 16,* p. 7.

9 Google Australia, *Submission 23*, p. 2.

4.11 Google also noted the scale of the problem, as well as how foreign state actors are engaging in CIB. Google stated that it tracks more than '270 targeted or government-backed attacker groups from more than 50 countries'.[10] Based on research from its Threat Analysis Group, which releases quarterly bulletins on its findings, Google described recent coordinated influence operations that it had detected:

> For the first quarter of 2020, we reported disabling influence campaigns originating from groups in Iran, Egypt, India, Serbia and Indonesia . Since March, 1 we've removed more than a thousand YouTube channels that were apparently part of a large campaign and that were behaving in a coordinated manner. These channels were mostly uploading spammy, non-political content, but a small subset posted primarily Chinese-language political content supporting Chinese Communist Party (CCP) policy and propaganda positions, similar to the findings of a recent Graphika report.[11]

4.12 Google further explained the motivations behind some of these activities, which can be both financially and politically driven:

> These groups have different goals in carrying out their operations: while security attacks may focus on collecting intelligence or stealing intellectual property, coordinated influence operations and disinformation campaigns may be financially motivated, engaging in disinformation activities for the purpose of turning a profit; others are politically motivated, engaging in disinformation to foster specific viewpoints among a population, to exert influence over political processes, or for the sole purpose of polarising and fracturing societies.[12]

4.13 Similarly, in its submission, Twitter noted the challenges that the platform faced in combatting foreign interference and other CIB:

> It is clear that information operations and coordinated inauthentic behavior will not cease. These types of tactics have been around for far longer than Twitter has existed. They will adapt and change as the geopolitical terrain evolves worldwide and as new technologies emerge. Given this, the threat we face requires extensive partnership and collaboration with government entities, civil society experts, and industry peers. We each possess information the other does not have, and our combined efforts are more powerful together in combating these threats.[13]

4.14 CIB is already occurring in Australia, with confirmed examples originating from domestic and international sources. Facebook noted that it had detected four examples of CIB occurring in Australia, including:

---

[10] Google Australia, *Submission 23*, p. 2.

[11] Google Australia, *Submission 23*, p. 2.

[12] Google Australia, *Submission 23*, pp. 2-3.

[13] Twitter, *Submission 20*, p. 6.

- in March 2019, a CIB operation originating from Macedonia and Kosovo, targeting countries around the world including Australia;
- in March 2019, a domestic CIB network was linked to local political actors in New South Wales;
- in October 2019, a CIB network was linked to marketing firms based in the United Arab Emirates, Nigeria and Egypt that was targeting public debate primarily in the Middle East and Africa, with some focus on Australia; and
- in August 2020, an English and a Chinese language CIB operation that acted primarily in English and in Chinese language criticised the Chinese government and spread misinformation about COVID-19.[14]

4.15 Significantly, Mr Nathaniel Gleicher, Global Head of Security Policy, Facebook highlighted that domestic actors are engaging in CIB, which in turn assists foreign powers engaged in the same behaviour:

> When we look at deceptive influence operations, CIB, about half of what we see is domestic in nature. While foreign interference is an important and very serious threat, we often see—as you described—foreign actors taking narratives from domestic actors, reflecting them or amplifying them, or we see entirely domestic operations using these techniques. In the conversation today, I think it is important to continue to focus on and tackle foreign interference, but we also have to think about what happens domestically. These are real citizens, from within our countries, that are driving these narratives. That tension is one that is going to continue to be a challenge for all of us, and we are seeing sophisticated foreign actors attempt to make themselves appear domestic and attempt to wander their narratives through domestic actors who may be sympathetic to their ideas.[15]

The attention economy

4.16 A key element to social media platforms' business models is the revenue that is produced through the selling of advertisements. This business model, which is founded on the capitalisation of user attention in order to sell advertisements, has been dubbed the 'attention economy'.[16]

4.17 Responsible Technology Australia described how the financial incentive for social media platforms to retain users' attention has resulted in undesirable outcomes:

> This 'attention economy' is powered by the unregulated and limitless collection of user's personal data … Through this, the digital platforms have built intimate and detailed profiles on their users that enables them to be targeted via their interests, their vices, and their vulnerabilities. This

[14] Mr Nathaniel Gleicher, Global Head of Security Policy, Facebook, *Committee Hansard*, 30 July 2021, p. 3.

[15] Mr Nathaniel Gleicher, Facebook, *Committee Hansard*, 30 July 2021, p. 3.

[16] Responsible Technology Australia, *Submission 17*, p. 2.

> information is then used by the platform's algorithms to feed tailored content that is calculated to have the greatest potential of keeping users engaged and on the platform. This content has been shown to lean toward the extreme and sensational, as it is more likely to captivate user attention.[17]

4.18 Dr Jake Wallis and Mr Thomas Uren, ASPI, likewise argued that the business model of social media companies is encouraging the spread of low-quality content and providing an environment that is primed for foreign interference and CIB to occur:

> Online, financial incentives are linked to audience size—views, eyeballs, or clicks—and sensationalist and provocative content gathers more engagement, so content producers are de facto encouraged to produce sensationalist content, not necessarily high-quality journalism or even journalism of any sort.
>
> The governance models and ethics that previously applied to traditional journalism have been replaced on social media; absent restraining forces, the default profit-maximising behaviour for social media platforms is to allow sensationalist, provocative content. In this social media ecosystem foreign interference and malign actors can flourish.[18]

4.19 The data collected to fuel advertising sales also poses security risks. Ms Katherine Mansted described how the mass collection of user data, which is used to sell highly targeted advertisements, ultimately poses a security risk:

> The first is that all of us already leave a huge data residue behind us in everything that we do, and it is becoming increasingly possible for actors of all kinds—from the more benign, like marketers, to political campaigns in democratic countries—to understand intimately who we are and what makes us tick. If those actors can do it, so too can malign foreign state actors.[19]

4.20 Indeed, the low cost of advertisements on social media platforms hold significant appeal for foreign actors, particularly given the platforms' huge audience base. Dr Michael Jensen, Associate Professor, Institute for Governance and Policy Analysis, University of Canberra, noted the relatively low cost for foreign actors to place advertisements on Facebook:

> Meanwhile, we know that the Facebook content during the 2016 election reached 126 million people and it cost less than $100,000 for the ads that [Russia] put out there. Their Twitter operations cost a little over $1 million a month, but that's still not that much compared to what countries spend

---

17 Responsible Technology Australia, *Submission 17*, p. 2.

18 Jake Wallis and Mr Thomas Uren, ASPI, *Submission 2*, p. 5.

19 Ms Katherine Mansted, *Committee Hansard*, 22 July 2020, p. 20.

> on intelligence operations. It scales up much faster. Additionally, they can be much more adaptive.[20]

4.21 Dr Carlo Kopp warned that as long as social media companies continued to utilise a business model that rewards such 'clickbait' content, social media platforms will remain susceptible to hostile influence attacks.[21]

4.22 Despite social media platforms' business model being entirely based on utilising users' data to sell advertisements, much of their user base does not approve of these activities. Indeed, the Attorney-General's Department noted the ACCC's finding that '83 per cent of digital platform users were of the view that it was a misuse of their personal information when entities monitor and collect their personal information without express consent'.[22]

Secondary markets

4.23 Aside from the selling of advertising, secondary markets have also emerged on social media platforms, some of which are being used to facilitate CIB. One method is for malign actors to buy social media accounts in order to have a credible presence for engaging in CIB. Dr Jake Wallis and Mr Thomas Uren, Senior Analyst, ASPI, outlined their research regarding the proliferation of state-backed accounts spreading content on Twitter.[23] Dr Wallis noted that older accounts were being on-sold for malicious purposes:

> When we looked at Twitter's takedown data in September of last year, we could see that they were tweeting about issues as diverse as Indonesian IT tech support; they were tweeting in a huge range of languages. But, when you look at that dataset over time, you can see there's a particular point at which they start tweeting in Chinese. That suggests to us that these are accounts that have been used, perhaps hired out, by these kinds of shadow actors within this shadow economy. They're hired out, they serve various PR campaigns, and then they become involved in a state sponsored campaign.[24]

4.24 Dr Wallis further explained that there was a 'huge market' for such accounts, as a credible history of activity on the platform made the accounts harder to detect as compared to entirely new accounts, which were more 'overtly suspicious' to Twitter's algorithms and to Twitter's site integrity team.[25]

---

[20] Dr Michael Jensen, Associate Professor, Institute for Governance and Policy Analysis, University of Canberra, *Committee Hansard*, 22 June 2020, p. 27.

[21] Dr Carlo Kopp, *Submission 21*, p. 10.

[22] Attorney-General's Department, *Submission 13*, p. 6.

[23] Dr Jake Wallis and Mr Thomas Uren, Senior Analyst, International Cyber Policy Centre, ASPI *Committee Hansard*, 22 June 2020, pp. 11-12.

[24] Dr Jake Wallis, ASPI, *Committee Hansard*, 22 June 2020, p. 11.

[25] Dr Jake Wallis, ASPI, *Committee Hansard*, 22 June 2020, p. 11.

4.25 Mr Nathaniel Gleicher, Facebook, described how another market had emerged, where in marketing agencies can be hired to run disinformation campaigns on behalf of actors who would not normally have the technological capability to engage in CIB:

> One that I think is worth calling out is an increasing use of marketing firms or PR agencies that are essentially running disinfo for higher businesses—you hire them and they run your disinformation campaign. …we've seen more use of them lately, in two ways. First, we're seeing actors that otherwise wouldn't have the resources or the skills to run an influence operation hiring a firm to do that for them. We've seen smaller local campaigns—for example, not long ago, in the Mexican election, a number of operations linked to smaller and local campaigns run by these firms. So I think—particularly as you're thinking about your upcoming elections—being aware of this tool that could be used domestically is important.[26]

4.26 Mr Gleicher further noted how the use of such marketing agencies makes locating the source of a CIB campaign difficult or impossible:

> …if a government or a bad actor hires a PR firm and they pay them, not on Facebook, and they don't communicate with them on our platforms, we may be able to track it back to the PR firm but we won't be able to make the connection to the actor behind it. So it's interesting to note that the late 2019 operation that I mentioned that targeted Australia was in fact linked to three separate marketing firms. We don't necessarily know who hired them, but, as the different investigative teams, in governments, in civil society and in industry, get better and better at exposing these campaigns, I think we should expect more actors to use PR firms and other intermediaries to hide their identity.[27]

Paid political advertising

4.27 Advertisements on some social media platforms can be purchased for political purposes, which is significant given the reach of social media platforms, particularly to groups who may not engage with traditional sources of media.[28] Rules about the acceptability of political advertisements vary significantly via platform, as the Department of Home Affairs noted:

> There is significant variation in each platform's stated position of the issue of 'disinformation', perhaps best exemplified by differences between Facebook and Twitter's stance on political advertising. Whereas Facebook does "not police the truthfulness" of political advertisements on its platform, Twitter has banned political advertising. Such differences also extend to definitions, policies, procedures and responses for dealing with cases of disinformation.[29]

---

[26] Mr Nathaniel Gleicher, Facebook, *Committee Hansard*, 30 July 2021, p. 3.

[27] Mr Nathaniel Gleicher, Facebook, *Committee Hansard*, 30 July 2021, p. 3.

[28] Professor Kerry McCallum, Director, News and Media Research Centre, University of Canberra, *Committee H*ansard, 25 September 2020, p. 1.

[29] Department of Home Affairs, *Submission 16*, p. 7.

4.28 Political advertising is permitted on Facebook, save when the company determines to restrict it prior to an election, as Facebook did before the 2019 Federal Election campaign.[30] Facebook highlighted this temporary restriction on political advertising as an example where it had 'limited the possibility of undue foreign influence in politics',[31] despite allowing such political advertising to routinely occur in non-election periods.

4.29 Facebook's paid political advertising processes have been questioned by the Law Society of New South Wales (NSW) Young Lawyers, which noted that even during this period of restricted advertising Facebook did not:

- require advertisers to pass an approval process before being able to run political advertisements;
- require advertisements to display a disclaimer showing the name and entity which paid for the advertisement; and
- make political advertisements publicly available in an archive.[32]

4.30 Additionally, the Law Society of NSW Young Lawyers noted that Facebook had disabled Political Ad Collector, a tool created by ProPublica, which had allowed users to access information showing why a user was targeted by a particular political advertisement and to view political advertisements on Facebook which were not aimed at their demographic group.[33] Facebook stated that it had disabled the tool because it 'did not want malicious third parties to scrape the user data harvested by the project'.[34]

4.31 Facebook has recently sought to reform its paid political advertising practices. As of August 2020, Facebook also applied further restrictions to political advertising on the platform. The organisation submitted:

> Anyone who wants to run a political ad needs to provide identification and be authorised by Facebook prior to running the ad. And political ads are mandated to remain archived in the Ad Library for up to seven years after they have run.[35]

4.32 Facebook is also planning to restrict paid political advertising prior to the upcoming Federal Election. Mr Josh Machin, Head of Policy, Australia, Facebook, stated:

> We've had particular requirements in place for political ads since last year; but, in the last month, we have expanded those, in preparation for an upcoming election, to also cover social issues. So that covers organisations

---

30 Law Society of New South Wales (NSW) Young Lawyers, *Submission 11*, p. 7

31 Facebook, *Submission 27*, pp. 17-18.

32 Law Society of NSW Young Lawyers, *Submission 11*, pp. 7-8.

33 Law Society of NSW Young Lawyers, *Submission 11*, p. 8.

34 Law Society of NSW Young Lawyers, *Submission 11*, p. 8.

35 Facebook, *Submission 27*, p. 17.

> that might be advocating on anything that's important to democracy—the economy, education, the environment, defence, whatever it might be—and they don't necessarily need to be a political candidate or a political party.
>
> The steps that we take in relation to those ads include undertaking an authorisation process, where people are required to provide us with identification that demonstrates that they are within Australia. We require them to put disclosures on all of those ads, so the public can see who is funding them, where it's come from.[36]

4.33 Google, which also owns YouTube, allows for paid political advertising on its platforms. Mrs Lucinda Longcroft, Director, Government Affairs and Public Policy, Australia and New Zealand, Google Australia, described the company's activities in this area:

> With regard to elections, we provide regular training for members and senators, for staff and for the political parties to ensure that they understand the use of our tools with regard to elections. ... We work, as I mentioned, with the Australian Electoral Commission to ensure that election information is accurately and widely displayed on our platforms, and we have fairly recently developed a new electoral ad transparency program within Australia which requires that persons or organisations funding ads with a political intent based in Australia are Australian citizens or nationals or have permanent residency, and the funder of any ad must be disclosed on that ad itself.[37]

4.34 Facebook and Google's approach to paid political advertising differs from other social media platforms. TikTok does not allow paid political advertising on its platform,[38] and WeChat has likewise prohibited paid promotional content regarding:

- a candidate for an election; a political party; or any elected or appointed government official appealing for votes for an election;
- appeals for financial support for political purposes; and
- a law, regulation or judicial outcome, including changes to any such matter.[39]

4.35 From October 2019, Twitter has banned paid political advertising.[40] Ms Kara Hinesley, Director of Public Policy, Australia and New Zealand, Twitter,

---

[36] Mr Josh Machin, Head of Policy, Australia, Facebook, *Committee Hansard*, 30 July 2021, p. 8.

[37] Ms Lucinda Longcroft, Director, Government Affairs and Public Policy, Australia and New Zealand, Google Australia, *Committee Hansard*, 30 July 2021, p. 13.

[38] TikTok, *Submission 26*, p. 4.

[39] WeChat, *Submission 30*, [p. 3].

[40] Twitter, *Submission 20.1*, p. 4.

described the company's rationale behind this decision, noting in particular the view that political messages should be 'earned, not bought': [41]

> On 30 October 2019, our CEO announced that Twitter would stop all political advertising globally. We remain the only platform to date to implement a ban on political advertising. We believe the reach of political messages should be earned, not bought. This means bringing ads from political candidates and political parties to an end. Our approach to political advertising does not compromise free expression, because candidates and political parties can still share their content organically. This policy is focused on addressing the types of problems from paying for the reach of political speech to audiences on Twitter, which we believe has significant ramifications for democratic infrastructures online.[42]

Undermining of democratic institutions

4.36 The undermining of democratic institutions was raised as an issue by a number of submitters, who were concerned by the role social media was playing in the erosion of public trust in traditional institutions and in the integrity of Australia's elections. The Department of Home Affairs observed that 'social media can be a particularly effective tool in the manipulation of information'.[43] The Department noted that hostile foreign actors actively use social media to promote narratives and spread disinformation, which serves these actors' strategic interests, whilst undermining democratic processes and institutions, and stifling dissenting voices.[44]

4.37 Further, the department warned that 'if left unchecked, foreign interference can exploit Australia's way of life and open system of government to erode our sovereignty'.[45] It stated that acts of foreign interference can 'limit the Australian polity's ability to make independent judgements and can corrupt the integrity of Australia's systems'.[46] The department concluded that such acts can also erode public confidence in Australia's political and government institutions and can interfere with private sector decision-making to the detriment of Australia's national security and economic prosperity.[47]

4.38 Other submitters agreed with this assessment. Twitter submitted that '[f]oreign interference is an unavoidable part of a globalised communications

---

[41] Ms Kara Hinesley, Director of Public Policy, Australia and New Zealand, Twitter, *Committee Hansard*, 30 July 2021, p. 48.

[42] Ms Kara Hinesley, Twitter, *Committee Hansard*, 30 July 2021, p. 48.

[43] Department of Home Affairs, *Submission 16*, p. 3.

[44] Department of Home Affairs, *Submission 16*, p. 3.

[45] Department of Home Affairs, *Submission 16*, p. 3.

[46] Department of Home Affairs, *Submission 16*, p. 3.

[47] Department of Home Affairs, *Submission 16*, p. 3.

landscape'[48] and that foreign actors are acting to 'exploit social tensions, amplify polarisation, and undermine trust and confidence in democratic norms, institutions, and values'.[49] However, Twitter did note that, to date, it had 'not observed any foreign manipulation or foreign malicious activity related to suppression or interference with an election in Australia'.[50]

4.39 On the issue of long-term erosion of public trust in governments, political leadership and public institutions, Dr Michael Jensen noted that this growing distrust was also being exacerbated by a decline in the domestic political discourse:

> … it's not just a matter of citizens acting poorly or social media platforms failing to police themselves. Politicians therefore need to take responsibility for protecting the information environment as well. In fact, our survey data reveals, as Kerry mentioned, that Australians are considerably more worried about misinformation spread by their own politicians than they are about malign foreign actors. …
>
> Research in political science shows that elites play a significant role in agenda setting and setting the terms of debate for their supporters. Research also shows that one of the most powerful ways to shut down the spread of misinformation is for political leaders to denounce an otherwise politically convenient distortion or lie. But when they repeat those statements or at least admit them as legitimate issues for consideration they give them legitimacy, and that allows them to spread much further.[51]

4.40 Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, noted this same issue, stating that '[t]here are recurrent indications that Australians, irrespective of economic circumstances or education, distrust politicians and are disengaging from political processes'.[52] In order to combat this effect, the submitters proposed the introduction of an anti-corruption agency and increased transparency in political activities.[53]

The 2019 Federal Election

4.41 A number of submitters were concerned about the conduct of the 2019 Federal Election,[54] despite the Joint Standing Committee on Electoral Matters' *Report on*

---

48 Twitter, *Submission 20*, p. 8.

49 Twitter, *Submission 20*, p. 8.

50 Ms Kara Hinesley, Twitter, *Committee Hansard*, 30 July 2021, p. 48.

51 Dr Michael Jensen, *Committee Hansard*, 25 September 2020, p. 3.

52 Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, *Submission 7*, [p. 9].

53 Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, *Submission 7*, [p. 9].

54 Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, *Submission 7*, [p. 5]; Law Society of NSW Young Lawyers, *Submission 11*, p. 4; Responsible Technology Australia, *Submission 17*, pp. 9-14; Law Council of Australia, *Submission 18*, p. 20; and Australia Institute, *Submission 31.1*, p. 10.

the conduct of the 2019 federal election and matters related thereto finding that 'there was no foreign interference, malicious cyber-activity or security matters that affected the integrity of the 2019 Federal election'.[55] The report further stated that the committee 'found limited evidence of social media manipulation within Australia, including minimal use of bots',[56] although it did warn that 'given the significant rise in organised social media manipulation campaigns, we must remain vigilant'.[57]

4.42 The Electoral Integrity Assurance Taskforce's agencies likewise 'did not identify foreign interference nor any other interference that compromised the delivery of the 2019 Federal election or would undermine the confidence of the Australian people in the electoral process'.[58]

4.43 However, several submitters were still concerned about the integrity of the 2019 Federal Election. The annex of Responsible Technology Australia's submission provides examples of alleged misinformation and CIB in an Australian context, including a Queensland University of Technology study that concluded that there were a substantial number of bots that were tweeting content related to the 2019 Federal Election.[59] Responsible Technology Australia submitted:

> A [Queensland University of Technology] study which examined around 54,000 accounts out of more than 130,000 Twitter users active, during and after the 2019 Australian Federal Election (looking at over 1 million tweets) revealed that 13% of accounts were 'very likely' to be bots, with the majority originating from New York. This is estimated to be more than double the rate of bot accounts in the US presidential election.[60]

4.44 Responsible Technology Australia also cited the spread of false information on WeChat in May 2019, with reference to alleged anti-Labor and anti-Liberal propaganda.[61] This included posts that criticised Australia's involvement in the

---

[55] Joint Standing Committee on Electoral Matters (JSCEM), *Report on the conduct of the 2019 federal election and matters related thereto*, December 2020, p. 112. This finding was affirmed by Mr Neil Hawkins: Mr Neil Hawkins, Acting Deputy Coordinator and Acting First Assistant Secretary, National Counter Foreign Interference Coordination Centre, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 6.

[56] JSCEM, *Report on the conduct of the 2019 federal election and matters related thereto*, December 2020, p. 112.

[57] JSCEM, *Report on the conduct of the 2019 federal election and matters related thereto*, December 2020, p. 112.

[58] Department of Home Affairs, *Submission 16*, p. 6.

[59] Responsible Technology Australia, *Submission 17*, pp. 9-14 (Australian examples) and pp. 15-17 (international examples). Law Council of Australia, *Submission 18*, pp. 8-10 also provides international examples of foreign interference via social media.

[60] Responsible Technology Australia, *Submission 17*, p. 9.

[61] Responsible Technology Australia, *Submission 17*, pp. 9-10 and pp. 12-13.

Five Eyes alliance.[62] Responsible Technology Australia also cited the ability of political parties and lobbying groups to spend unchecked amount of monies of social media platforms,[63] and the spread of potentially inaccurate information on WeChat.[64]

4.45 The Law Council of Australia noted that during April and May 2019, Facebook temporarily prohibited political or electoral advertisements that were purchased from outside Australia, whereby advertisements from foreign entities that contained references to politicians, parties or election suppression, or political slogans or party logos were banned.[65] The Law Council of Australia also further explained the Australian Electorate Commission's difficulties with Facebook during this period:

> During 2019, it was reported that Facebook had not adequately applied the authorisation rules set out by the Electoral Act to advertising on its platform and did not respond to AEC inquiries about the source of advertising in a timely manner. Facebook's reported response was firstly that the advertising in question was not paid advertising and therefore was not required to comply with the authorisation requirements under Part XXA. Four weeks after AEC first raised the issue with Facebook, it was agreed that the Page was paying for advertisements, however by this stage the group had already been removed by the administrator.[66]

4.46 The Australia Institute was likewise concerned by Facebook's conduct during the 2019 Federal Election:

> Because there is very little incentive or material consequences for ensuring an accurate and truthful election campaign process, platforms such as Facebook have failed to address suspicious and fraudulent political activity, including several incidents on political advertising integrity both in the lead up to and during the 2019 Federal Election.[67]

Social polarisation

4.47 Social polarisation is a term used to describe increasing a segregation of views within a given society. The increase of social polarisation, as facilitated by social media, was raised by several submitters as a particularly pernicious issue. In describing this effect, Dr Mathieu O'Neil, Associate Professor of Communication, News and Media Research Centre, University of Canberra, stated that 'the aim of foreign agencies is to emphasise divisions in society, to

---

62 Responsible Technology Australia, *Submission 17*, p. 13.

63 Responsible Technology Australia, *Submission 17*, p. 11.

64 Responsible Technology Australia, *Submission 17*, pp. 11-13.

65 Law Council of Australia, *Submission 18*, p. 20 and p. 23. See also Responsible Technology Australia, *Submission 17*, p. 10.

66 Law Council of Australia, *Submission 18*, p. 32.

67 Australia Institute, *Submission 31.1*, pp. 10-11.

pit groups against each other'.[68] The committee was given evidence from Dr Carlo Kopp that proxy groups such as activists are used in a similar fashion to how the Soviet Union employed print media and broadcast radio to spread disinformation leading to social division:

> Another feature of the COVID-19 / SARS-CoV-2 "deception pandemic" is the extensive use of proxy groups, comprising both activists and supporters, to promote and propagate deceptive narratives and claims in both social and mass media. The employment of agenda driven domestic entities to cause mayhem and disruption is not a new phenomenon and arguably is an extension of the subversion techniques developed by the Soviets during the interwar period to induce regime change. Indeed, most of the foreign influence practices conducted in digital media by adversaries of Western democracies are no more than a "digital refresh" of classic Komintern and Soviet propaganda, disinformation, and subversion techniques, widely employed during the Cold War using print media and broadcast radio.[69]

4.48 While social polarisation has been increasing, it ought to be noted that not all social polarisation online is inauthentic or a result of CIB. Mr Lachlan Colquhoun, First Assistant Secretary, Department of the Prime Minister and Cabinet noted the difficulty of determining what was the result of state-driven activity, as opposed to organically emerging movements, and referred to the difficulty in proving which was which.[70]

4.49 In describing how social polarisation occurs online, Ms Katherine Mansted stated that social media platforms 'often amplify divisive and emotionally charged content'[71] and that 'the business models of these particular platforms rest on attention, and, therefore, emotion sells'.[72] Responsible Technology Australia likewise submitted that 'divisive, sensationalist clickbait has been shown to spread faster online, allowing foreign actors to be able to "game" this system and peddle mass amounts of content with the intention of driving polarisation'.[73]

4.50 In their submission, the Allens Hub for Technology, Law and Innovation; the Datafication and Automation of Human Life; and the Society on Social Implications of Technology (Allens Hub et al) described how such social polarisation can occur:

---

[68] Dr Mathieu O'Neil Associate Professor of Communication, News and Media Research Centre, University of Canberra, *Committee Hansard*, 25 September 2020, p. 4.

[69] Dr Carlo Kopp, *Submission 21*, pp. 8-9.

[70] Mr Lachlan Colquhoun, First Assistant Secretary, Department of the Prime Minister and Cabinet, *Committee Hansard*, 11 December 2020, p. 14.

[71] Ms Katherine Mansted, *Committee Hansard*, 22 June 2020, p. 17.

[72] Ms Katherine Mansted, *Committee Hansard*, 22 June 2020, p. 17.

[73] Responsible Technology Australia, *Submission 17*, p. 3.

> Platforms know that users tend to be more engaged with a platform when shown more extreme and controversial content. When this is built into an algorithm, it tends to drive people to content reflecting more extreme versions of their own views. … Because social media platforms in particular prioritise content generated or liked by friends, it is easy to fall into 'filter bubbles' where a user is only exposed to content that reflects their existing world-views.[74]

4.51 To consider one specific example, the Australian Muslim Advocacy Network (AMAN) raised the issue of rising Islamophobia in Australia, which it views as rhetoric that has been imported from the United Kingdom, Europe and United States of America to Australia via coordinated exercises on social media platforms like Facebook.[75] In its submission, AMAN cited a December 2019 investigation by *The Guardian Australia* that had concluded that an overseas commercial enterprise was 'using its 21-page network to churn out more than 1,000 coordinated faked news posts per week to more than 1 million followers, funnelling audiences to a cluster of 10 ad-heavy websites and milking the traffic for profit'.[76] The material utilised was Islamophobic in nature and vilified specific Muslim politicians.[77]

4.52 Dr Jake Wallis, ASPI, also discussed investigations into Islamophobia during late 2019:

> Back in 2019, in the lead-in to the federal election, there were substantial audiences in Facebook groups that were managed from Kosovo, the Republic of North Macedonia and Albania that were being fed an ongoing selection of Islamophobic content. That was driving engagement, which was reasonably sustained. I think we had audiences of about 130,000 across those Facebook groups. The aim for those actors is to drive engagement and then they will provide links within those groups, when they have that substantial audience, and they will steer those audiences to content farms, websites, outside of Facebook that will serve advertising. The serving of advertising generates revenue for the individuals behind the websites.[78]

4.53 Dr Wallis further noted that these actors may not be solely financially motivated and that there was 'often an overlap of political ideology and

---

74 Allens Hub for Technology, Law and Innovation; the Datafication and Automation of Human Life; and the Society on Social Implications of Technology (Allens Hub et al), *Submission 19*, pp. 2-3

75 Australian Muslim Advocacy Network (AMAN), *Submission 24*, p. 1.

76 AMAN, *Submission 24*, p. 1.

77 AMAN, *Submission 24*, p. 1.

78 Dr Jake Wallis, ASPI, *Committee Hansard*, 22 June 2020, p. 13. See also Dr Jake Wallis and Mr Thomas Uren, ASPI, *Submission 2*, p. 1.

financial motivation',[79] as the financial benefit of their activities allowed them to further their ideologically-based activities.[80]

4.54 Responsibly Technology Australia also discussed the rise in Islamophobic content, noting that a network of Facebook pages that were run out of the Balkans had profited from the manipulation of Australian public sentiment, by using 'hot button issues such as Islam, refugees and political correctness, [to drive] clicks to stolen articles in order to earn revenue from Facebook's ad network'.[81] Responsibly Technology Australia specifically identified the 'Australians against Sharia' page, which has over 67,000 members, as one of the most prominent pages in the network.[82]

4.55 In response to the rising issue of social polarisation, Dr Richard Johnson, First Assistant Secretary, Social Cohesion Division, Department of Home Affairs, described how the Department of Home Affairs was attempting to 'strengthen Australia's social cohesion' by promoting the uptake of citizenship and democratic values and attempting to increase community resilience.[83]

4.56 In contrast to other submitters, Mr Nathaniel Gleicher, Facebook, downplayed the polarising role of social media:

> … the research on the impact that social media has on polarisation is actually much more uncertain than we often say. There are studies suggesting that it can help reduce polarisation and there are studies suggesting that it can help contribute to it. There are also a lot of studies saying it is driven by what's happening in broadcasting and other spaces. So one of the keys in trying to tackle this is just to recognise that the threat actors are targeting the entire media ecosystem—broadcast, social media and public debate.[84]

Social media as a source of news

4.57 Social media is increasingly a source of news for many Australians, despite the lack of regulation and fact-checking of content on the platforms. An issue raised by several submitters was the tendency of global populations, including Australians, to access news via social media platforms, as opposed to more traditional news sources, such as newspapers, television and radio.

---

79 Dr Jake Wallis, ASPI, *Committee Hansard*, 22 June 2020, p. 13.

80 Dr Jake Wallis, ASPI, *Committee Hansard*, 22 June 2020, p. 13.

81 Responsibly Technology Australia, *Submission 17*, p. 11.

82 Responsibly Technology Australia, *Submission 17*, p. 11.

83 Dr Richard Johnson, First Assistant Secretary, Social Cohesion Division, Department of Home Affairs described how the Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 9 and p. 2.

84 Mr Nathaniel Gleicher, Facebook, *Committee Hansard*, 30 July 2021, p. 9.

4.58 The University of Canberra's 2021 *Digital news report* noted that '[t]he decline in TV and print news is emblematic of the gradual shift away from traditional news platforms towards online and social media news sources'.[85] Mr Robert McKinnon, Assistant Secretary, Department of Foreign Affairs and Trade (DFAT), also raised that, for some countries within Australia's region, Facebook is the primary vehicle for news,[86] as opposed to more traditional sources of news media.

4.59 Professor Kerry McCallum, Director, News and Media Research Centre, University of Canberra, likewise noted the increasing role of social media as a news source, especially for Australians who already have low news literacy:

> I can highlight three interconnected findings from our research. Firstly, Australians are increasingly relying on social media for their news. While television is still the main source of news for most people, 52 per cent of us use social media as a general source of news and 21 per cent use it for their main source of news; 39 per cent of us use Facebook to access news. Secondly, Australians have low levels of news literacy compared to other countries. In our 2018 report; we found that 58 per cent of Australians have low news literacy. Significantly, 76 per cent of those who rely on social media for news have low news literacy.[87]

4.60 Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, highlighted that 'social media platforms are now significant mechanisms for the dissemination of information in Australia about political parties and individual politicians, public policy issues and local/international events'.[88] Dr Arnold and Dr Sheehy considered that the significance of social media platforms in this area has four bases:

- the social nature: they are more trusted than 'official' sources;
- the replacement of mainstream media;
- weak regulation and a lack of editorial control; and
- the validation social media platforms can provide to users.[89]

4.61 Ms evelyn douek noted that some overseas disinformation campaigns seek to 'sow the idea of distrust and apathy about public discourse more generally'.[90]

---

85 See Sora Park, Caroline Fisher, Kieran McGuinness, Jee Young Lee, and, Kerry McCallum, *Digital news report: Australia 2021*, June 2021, p. 10.

86 Mr Robert McKinnon, Assistant Secretary, Department of Foreign Affairs and Trade (DFAT), *Committee Hansard*, 11 December 2020, p. 18.

87 Professor Kerry McCallum, Director, News and Media Research Centre, University of Canberra, *Committee H*ansard, 25 September 2020, p. 1.

88 Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, *Submission 7*, pp 3-4.

89 Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, *Submission 7*, pp 3-4.

90 Ms evelyn douek, *Committee Hansard*, 22 June 2020, p. 5.

Similarly, Dr Michael Jensen observed that the decline in trust in news in Australia had resulted in negative consequences:

> … trust in news is critical to a functioning democracy—but trust in Australia's news has been declining. … foreign actors can exploit declining trust in professional journalism in order to polarise society and undermine Australia's capacity for self-governance. News sources play a central role in the construction of a citizen's information environment, and social media are increasingly important sources through which persons are accessing information.[91]

4.62 Dr Jensen further explained how the spread of misinformation and erosion of trust in traditional news sources can have serious impacts on public life:

> News media fragmentation and political polarisation go hand in hand to create unique vulnerabilities that foreign actors can use to manipulate the public as well as our political authorities. Fragmentation and publicly available sets of information and contextual understandings in political life open fissures in the information environment that foreign actors can exploit and use against us. Without a common set of facts, it's hard to move people to a common set of ends.[92]

4.63 Professor Kerry McCallum, University of Canberra, noted the need for 'a concerted effort to improve media literacy across the Australian constituency',[93] as did the Australia Institute.[94] Dr Jake Wallis and Mr Thomas Uren, ASPI, likewise raised the importance of traditional media sources in this context:

> The issues that malign actors use to drive division, to influence and manipulate audiences at scale may not even be overtly political. As hierarchical models of information distribution (from government, from national broadcasters, from mainstream media) are replaced by a proliferation of information flows, trusted networks become increasingly important as sources of reliable content.[95]

4.64 This state of affairs may be improving. The University of Canberra's 2021 *Digital news report* found that, over the past 12 months, trust in news had risen in Australia to 43 per cent, a five per cent improvement of figures from the previous year. The report observed that '[t]he improvement in trust likely reflects the public's greater reliance on news in a crisis, and the active dissemination of official health advice by news outlets during the pandemic.'[96]

---

91 Dr Michael Jensen, *Committee Hansard*, 25 September 2020, p. 2.

92 Dr Michael Jensen, *Committee Hansard*, 25 September 2020, p. 2.

93 Professor Kerry McCallum, University of Canberra, *Committee Hansard*, 25 September 2020, p. 2.

94 Australia Institute, *Submission 31*, p. 17.

95 Dr Jake Wallis and Mr Thomas Uren, ASPI, *Submission 2*, p. 3.

96 Sora Park, Caroline Fisher, Kieran McGuinness, Jee Young Lee, and, Kerry McCallum, *Digital news report: Australia 2021*, June 2021, p. 9.

4.65 However, the 2021 *Digital news report* also found that concern about false and misleading information in Australia is high (64 per cent) and higher than the global average (56 per cent). Fifty-nine per cent of Australians reported that they had encountered misinformation in the week prior to the survey being undertaken. The report expanded on this finding:

> Across a range of topics, experience of misinformation about COVID-19 was the highest (38%) followed by politics (33%) and climate change (29%). Nearly a quarter of participants did not know if they had come across misinformation (23%). This figure is higher among those with low education (30%), indicating a lack of awareness or ability to identify misinformation.[97]

4.66 In contrast, some submitters expressed concern that governments may impose arbitrary regulations to address the issue of fake news, which they viewed as eroding civil liberties and free speech.[98] For example, the Australian Citizens Party submitted that the 'risk posed to Australia's democracy by foreign interference through social media' is minimal, and does not warrant the 'extreme policy responses' that have been proposed to mitigate it, either in Australia or internationally.[99]

Targeting of journalists

4.67 Poor news practices on social media platforms are having impacts on journalists, who may be impersonated or deceived on social media platforms. Google observed that, since the beginning of 2020, a rising number of attackers had been impersonating news outlets and journalists, seeking to seed false stories with other reporters to spread disinformation.[100] Foreign Policy experts were also being targeted by attackers seeking to access their research, organisations they work for, and fellow researchers.[101]

4.68 Mr Nathaniel Gleicher, Facebook, described how legitimate journalists can be deceived into writing inauthentic content:

> One of the new techniques we see increasingly is that actors, particularly those linked to Russia and Iran, are directly reaching out to reporters around the world, trying to trick them into writing the stories for them, the idea being that, if you can get a reporter to write your false narrative, you already get a whole bunch of public awareness. We've seen this be successful in the United States.[102]

---

97 Sora Park, Caroline Fisher, Kieran McGuinness, Jee Young Lee, and, Kerry McCallum, *Digital news report: Australia 2021*, June 2021, p. 9.

98 Ms Melissa Harrison, *Submission 5*, p. 1; and the Australian Citizens Party, *Submission 9*, p. 1.

99 Australian Citizens Party, *Submission 9*, p. 1.

100 Google Australia, *Submission 23*, p. 4.

101 Google Australia, *Submission 23*, p. 4.

102 Mr Nathaniel Gleicher, Facebook, *Committee Hansard*, 30 July 2021, p. 4.

4.69 Mr Gleicher further outlined a concerning situation where journalists were being hired by false media organisations:

> … there are people who are, unfortunately, tricked into working for one of those campaigns. We've seen Russian actors run false media organisations. One of the most prominent examples is that they ran two false media organisations targeting, among other places, the United States, one aimed at the far Right and the other aimed at the far Left. They hired local reporters or freelancers who didn't know any better to write for them, trying to make their voices appear more authentic and trying to have more impact.[103]

Transparency

4.70 Currently, social media platforms determine what materials are publicly released regarding the content on their platforms and the activities they undertake, including content moderation policies, use of user data and the nature of the algorithms used. Witnesses have noted this lack of transparency has created difficulties in discerning the internal functioning of social media companies and whether their responses to foreign interference, misinformation, disinformation and CIB occurring on their platforms have been adequate.[104]

4.71 Ms evelyn douek noted that social media platforms have been reluctant to release information regarding content moderation and the removal of disinformation and misinformation:

> How successful have platforms been in adopting these [takedown] policies? We simply don't know. The data that platforms have released is relatively sparse. Some of the figures that platforms have released about takedowns sound impressive, but it's important to emphasise we don't know what these truly represent as a percentage of misinformation on these platforms, nor do we know how much unproblematic content was swept up in these removals. The only thing we know for certain, from experience, is that there will have been some measure of both over- and under-enforcement of misinformation courses.[105]

4.72 AMAN noted that due to a lack of transparency requirements in Australia, 'it is not possible to ask Facebook to reveal if a Page is run by who it claims to be run by, even if it is in public interest or important to running a civil remedy claim'.[106]

---

[103] Mr Nathaniel Gleicher, Facebook, *Committee Hansard*, 30 July 2021, p. 4.

[104] See Dr Jake Wallis and Mr Thomas Uren, ASPI, *Submission 2*, pp. 5-6; Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, *Submission 7*, p. 7; Responsible Technology Australia, *Submission 17*, p. 1; AMAN, *Submission 24*, p. 2; Principle Co, *Submission 25*, p. 7; Law Council of Australia, *Submission 18*, p. 1 and p. 30; and Ms evelyn douek, *Committee Hansard*, 22 June 2020, p. 2.

[105] Ms evelyn douek, *Committee Hansard*, 22 June 2020, p. 2.

[106] AMAN, *Submission 24*, p. 2.

4.73 Many submitters raised the necessity of transparency and the need for more information to be released to the public. Dr Jake Wallis and Mr Thomas Uren, ASPI, submitted that social media companies should be required to make their content moderation policies and enforcement actions transparent, including publicly releasing content moderation guidelines and regular transparency reports.[107] Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, likewise recommended the institution of a transparency regime,[108] as did Responsible Technology Australia.[109]

4.74 The Law Council of Australia stated that increased transparency would need to be 'proportionate, reasonably appropriate and adapted to address the legitimate threat of disinformation and foreign interference'[110] and outlined materials that, in its view, ought to be released publicly:

> Requirements, legislative or otherwise, which would mandate social media platforms to establish public databases of political advertisements, which present data such as the amount spent on the advertisements, and by whom the money was spent, and targeting parameters, would be an important and significant step forward.[111]

4.75 Social media companies have voluntarily undertaken some transparency measures, despite the lack of any formal requirement that they do so. Facebook submitted that it undertakes quarterly reporting on Community Standards Enforcement and monthly reporting on the removal of coordinated inauthentic behaviour.[112] It has also established an Ad Library, which catalogues 'all active ads any Page is running, along with more Page information such as creation date, name changes, Page merges and the primary country of people who manage Pages with large audiences'.[113]

4.76 TikTok noted the public availability of its terms of service, privacy policy, and community guidelines, which it uses to provide a 'safe and friendly environment' for users.[114] Google also publishes transparency reports, including one on misinformation and disinformation.[115]

4.77 Twitter noted that its activities in this area include:

---

[107] Dr Jake Wallis and Mr Thomas Uren, ASPI, *Submission 2*, pp. 5-6.

[108] Dr Bruce Arnold and Dr Benedict Sheehy, University of Canberra, *Submission 7*, p. 7.

[109] Responsible Technology Australia, *Submission 17*, p. 1.

[110] Law Council of Australia, *Submission 18*, p. 1.

[111] Law Council of Australia, *Submission 18*, p. 30.

[112] Facebook, *Submission 27*, p. 9.

[113] Facebook, *Submission 27*, p. 17.

[114] TikTok, *Submission 26*, p. 2.

[115] Mrs Lucinda Longcroft, Google Australia, *Committee Hansard*, 30 July 2021, p. 14.

- retrospective reviews of elections;[116]
- establishing an Ads Transparency Centre, which ' includes a repository of all advertisements served on Twitter within the last seven calendar days, as well as all of the political campaign ads paid for by certified political advertisers in Australia';[117] and
- a bi-annual Transparency Report.[118]

4.78 In 2018, Twitter also commenced archiving Tweets and media connected to potentially-state backed operations, which are publicly released:

> In line with our strong principles of transparency and with the goal of improving understanding of foreign influence and information campaigns, we release archives of Tweets and media associated with potential information operations that we had found on our service, including the 3,613 accounts we believe were associated with the activities of the Internet Research Agency on Twitter dating back to 2009. We made this data available with the goal of encouraging open research and investigation of these behaviors from researchers and academics around the world.[119]

4.79 In its supplementary submission, Twitter noted that this archive is 'the only public archive of its kind'[120] and now spans operations across 15 countries, including more than nine terabytes of media and 200 million Tweets.[121] Twitter further stated that these datasets have been used by 'thousands of researchers' to 'conduct their own investigations and share their insights and independent analyses with the world'.[122]

COVID-19 misinformation and disinformation: a case study

4.80 The COVID-19 pandemic has highlighted the spread of online misinformation, which has resulted in real world impacts and created significant challenges for governments managing the pandemic. Dr Jake Wallis, ASPI, summarised the current domestic and international situation in terms of COVID-19 misinformation and disinformation:

> The pandemic has created a perfect storm of information manipulation, with these state and non-state actors echoing each other's theories, tactics and techniques. COVID-19 has spread globally and has been used to prey upon people's fears and to drive engagement for malign purposes, be it to scam people, to drive conspiracy theories, for extremists to recruit, radicalise or proselytise, or simply by states trying to gain advantage. This

---

116 Twitter, *Submission 20*, p. 5.

117 Twitter, *Submission 20*, p. 5.

118 Twitter, *Submission 20*, pp. 5-6.

119 Twitter, *Submission 20*, p. 6.

120 Twitter, *Submission 20.1*, p. 7.

121 Twitter, *Submission 20.1*, p. 7.

122 Twitter, *Submission 20*, p. 7.

> activity can mobilise offline. It can drive real-world harms. For example, the conflation of 5G conspiracy theories has resulted in attacks on cell towers. It's worth noting that throughout 2019 the Kremlin-funded RT advanced the theory that 5G causes harm. We also note last week's warnings from ASIO on the rise of right-wing extremism driven by COVID-19.[123]

4.81 In the Australian content, Dr Michael Jensen described some examples of the misinformation that is occurring and the real-world impacts it is leading to:

> We need look no further than the anti-mask and lockdown protests in Melbourne that we've seen recently to see how misinformation can mobilise people in ways that undermine our capacity to govern. False information downplaying the risks of the COVID virus, questions about the health value of lockdowns and face masks and conspiracies that politicise these issues in a fight against a conspiracy to deny basic rights—these kinds of communications are easy to find online, and once they become a premise for behaviour they undermine our capacity to contain the COVID-19 pandemic.[124]

4.82 Mr Alex Stamos, Director, Stanford Internet Observatory, described some of the common themes he had seen in COVID-19 misinformation and disinformation in the United States context:

> Here in the United States, a lot of the COVID disinformation has been domestic. A lot of it has been from people who are motivated around antivax, who believe that everything's a conspiracy—Bill Gates, despite having more money than God, has got some kind of plan to use vaccines to get more money; I'm not exactly sure what their theory is. One of the most effective pieces of domestic disinformation in the United States was a video called Plandemic, which seems to be financially motivated—grifters who are pushing it to sell stuff. That has been very effective, much more effective than any foreign campaign that we've seen.[125]

4.83 Ms Katherine Mansted likewise noted that COVID-19 was acting as a misinformation accelerant:

> …it is my opinion that COVID-19 has very much been an accelerant and will continue to be an accelerant for propaganda and disinformation. There is a significant body of cognitive research which demonstrates that people are more susceptible to propaganda and disinformation in times of high anxiety and uncertainty. COVID-19—not just the acute health crisis but also the economic and social consequences that will continue to flow for some time—will create fertile ground for disinformation and propaganda. This is something that we've seen a number of actors take advantage of, such as state actors, peddling disinformation and trying to enhance social polarisation, and extremist groups.[126]

---

123 Dr Jake Wallis, ASPI, *Committee Hansard*, 22 June 2020, p. 10.

124 Dr Michael Jensen, *Committee Hansard*, 25 September 2020, pp. 2-3.

125 Mr Alex Stamos, Director, Stanford Internet Observatory, *Committee Hansard*, 22 June 2020, p. 7.

126 Ms Katherine Mansted, *Committee Hansard*, 22 June 2020, p. 16.

4.84 Dr Carlo Kopp also noted that the example of COVID-19 misinformation was illustrative of how quickly and widely misinformation can spread online:

> The chaos and disruption observed as a result of the failure to effectively contain misinformation, disinformation and malinformation in social media, and mass media, during the current COVID-19 / SARS-CoV-2 pandemic, provides a good indication of the damage foreign nation state actors can inflict with a very modest investment.[127]

4.85 However, much COVID-19 misinformation in Australia seems to be limited to English-language sources. Dr Richard Johnson, Department of Home Affairs, explained how, while there was misinformation spreading, it did not seem to be specifically targeted at culturally and linguistically diverse communities:

> We haven't identified a sustained campaign. Certainly, there is a lot of misinformation circulating in the environment about COVID and COVID-related issues. We haven't identified a particular campaign [in languages other than English], but there is a lot of interaction between us and communities, in terms of providing them with trusted sources of information. In particular, we are referring them back to the Department of Health and australia.gov.au and making sure that, where it's needed, that trusted source of information is also translated for communities so that they can understand what the facts are.[128]

4.86 Additionally, Mr Alex Stamos, Director, Stanford Internet Observatory, noted that the COVID-19 pandemic and the misinformation environment proliferating around it had created political opportunities for opportunistic governments:

> What we've seen from an online propaganda perspective is a bifurcation between online propaganda that is about supporting the actions of a government and then using COVID as a tool to tear down other governments, often as part of programs or a geopolitical strategy that has existed for years. So they are opportunistically grabbing onto COVID to execute on geopolitical goals that have always existed.[129]

4.87 However, it is not only government actors taking advance of the misinformation and disinformation surrounding COVID-19. Dr Jake Wallis, ASPI, noted that a large range of actors were utilising COVID-19 misinformation and disinformation, whether for financial, political or geostrategic motivations,[130] which may account for its vast proliferation.

4.88 Lastly, Dr Richard Johnson, Department of Home Affairs, noted that extremists were utilising the COVID-19 pandemic to amplify their message:

---

127 Dr Carlo Kopp, *Submission 21*, p. 11.

128 Dr Richard Johnson, Department of Home Affairs, *Committee Hansard*, 30 July 2021, p. 41. Dr Johnson further noted that the government has invested in community liaison officers, who have the capability to translate non-English language material.

129 Mr Alex Stamos, Director, Stanford Internet Observatory, *Committee Hansard*, 22 June 2020, p. 2.

130 Dr Jake Wallis, ASPI, *Committee Hansard*, 22 June 2020, p. 11.

> Some of the extremist milieu are using the pandemic, and also the response to the pandemic, to amplify some of their key narratives. In the extremist context, we have certainly seen instances where COVID related narratives, including misinformation, are playing out.[131]

Scale

4.89 The ability of social media platforms to detect COVID-19 disinformation and their willingness to publicly release such information are crucial for assessing the scale of the issue.

4.90 Regarding the scope of the problem, Dr Carlo Kopp noted that Australia, as with comparable nations abroad, was experiencing a 'deluge' of online misinformation relating to COVID-19.[132] Dr Kopp stated:

> The scope and scale of the misinformation, disinformation and malinformation being distributed globally during the COVID---19 / SARS---CoV---2 pandemic is unprecedented and without any doubt dwarfs the two previous benchmarks, the UK Brexit vote and the US 2016 Presidential Election. In part this reflects the global footprint of the viral pandemic, and in part it reflects nation state players concurrently targeting domestic and foreign audiences.[133]

4.91 Ms evelyn douek noted that, while each major platform has 'rolled out more aggressive misinformation policies specifically related to COVID-19',[134] this had not been without difficulties:

> In terms of broader lessons from this approach, while reception of these measures has been broadly positive, even in the relatively more scientific realm of health information and where evidence of harms should be easier to determine, defining misinformation has been difficult in some cases. Authoritative sources have sometimes conflicted with each other and at other times simply got things wrong, which is to be expected in a rapidly evolving situation of high uncertainty. This does, however, suggest caution in overlearning the lessons of the pandemic in terms of policing this information with a heavy hand across all categories of content.[135]

4.92 Facebook reported that, between April and June 2020 alone, it had removed over 7 million posts for spreading harmful misinformation about COVID-19, which included 'harmful claims, like drinking bleach cures the virus or that COVID-19 was caused by 5G'.[136] By 30 July 2021, Mr Josh Machin, Facebook, reported that Facebook had removed 18 million posts that included harmful misinformation relating to COVID-19, as well as fact-checking 167 million

---

131 Dr Richard Johnson, Department of Home Affairs, *Committee Hansard*, 30 July 2021, p. 40.

132 Dr Carlo Kopp, *Submission 21*, p. 3.

133 Dr Carlo Kopp, *Submission 21*, p. 5.

134 Ms evelyn douek, *Committee Hansard*, 22 June 2020, p. 2.

135 Ms evelyn douek, *Committee Hansard*, 22 June 2020, p. 2.

136 Facebook, *Submission 27*, p. 3 and p. 9.

posts and labelling them as false information.[137] Mr Machin also noted that in 2020 Facebook removed 110,000 pieces of harmful COVID-19 misinformation that originated in Australia.[138]

4.93 In its July 2020 supplementary submission, Twitter stated that it had 'removed thousands of Tweets around the globe for containing misleading and potentially harmful content' and that its automated systems 'have challenged approximately 4.3 million accounts which were targeting discussions around COVID-19 with spammy or manipulative behaviors'.[139]

4.94 The Australia Institute reported that, in a 2020 investigation conducted with the Queensland University of Technology, it had found evidence of 'coordinated COVID-19 misinformation and disinformation on Twitter, for either commercial or political purposes'.[140] The Australia Institute noted:

> In some ways, the spread of COVID-19 disinformation mimics the outbreak of the virus itself, with the disinformation amplified and given authenticity by the wider fringe community that spreads it after it has been introduced by the inauthentic actors. [141]

4.95 In Google's July 2020 submission to the inquiry, it reported that it had 'detected 18 million malware and phishing Gmail messages per day related to COVID-19, in addition to more than 240 million COVID-related daily spam messages'.[142] Furthermore, Google noted that some of these international attacks were backed by foreign actors:

> Google's [Threat Analysis Group] has specifically identified over a dozen government-backed attacker groups using COVID-19 themes as lure for phishing and malware attempts—trying to get their targets to click malicious links and download files, including in Australia [143]

4.96 On 30 July 2021, Mr Richard Salgado, Director, Law Enforcement and Information Security, Google, noted that the amount of COVID-19 misinformation and disinformation was 'voluminous' and included 'a lot of criminal activity'.[144] Mrs Lucinda Longcroft, Director, Government Affairs and Public Policy, Australia and New Zealand, Google Australia, noted that, since

---

137 Mr Josh Machin, Facebook, *Committee Hansard*, 30 July 2021, p. 4.

138 Mr Josh Machin, Facebook, *Committee Hansard*, 30 July 2021, p. 4.

139 Twitter, *Submission 20.1*, pp. 17-18.

140 Australia Institute, *Submission 31*, p. 2.

141 Australia Institute, *Submission 31*, p. 2.

142 Google Australia, *Submission 23*, p. 4.

143 Google Australia, *Submission 23*, p. 4.

144 Mr Richard Salgado, Director, Law Enforcement and Information Security, Google, *Committee Hansard*, 30 July 2021, p. 12.

the beginning of 2020, the Google has 'have removed around 800,000 videos from YouTube and over 275 million COVID apps from across our platforms'.[145]

Social media platforms' responses to COVID-19 misinformation and disinformation

4.97 Social media platforms are attempting to combat the rapid proliferation of COVID-19 misinformation and disinformation on their platforms, with varying levels of success. Many of the platforms described what activities they had been undertaking to the committee.

4.98 Ms Kara Hinesley, Twitter, described how Twitter has prioritised tackling misinformation 'based on the highest potential for harm', which included a particular focus on COVID-19 misinformation and disinformation.[146] Twitter has undertaken a number of activities in this area, including:

- a global expansion of the COVID-19 search prompt, which ensured that people on the platform 'are met with credible, authoritative content at the top of their search experience';[147]
- a curated event feature for COVID-19, which contained credible information and the latest facts about COVID-19;[148]
- providing a dataset to developers and researchers regarding the public conversation about COVID-19 in real-time;[149]
- increasing machine learning and automated moderation to take action on potentially abusive and manipulative content;[150]
- building systems that enable its team to continue to enforce its rules remotely around the world;[151]
- instituting a global content severity triage system to prioritise potential rule violations that ' present the biggest risk of harm';[152]
- executing daily quality assurance checks on content enforcement processes;[153]
- engaging with Twitter's partners around the world;[154]
- reviewing Twitter's rules in the context of COVID-19;[155]

---

145 Mrs Lucinda Longcroft, Google Australia, *Committee Hansard*, 30 July 2021, p. 12.

146 Ms Kara Hinesley, Twitter, *Committee Hansard*, 30 July 2021, p. 48.

147 Twitter, *Submission 20*, p. 9.

148 Twitter, *Submission 20*, p. 11.

149 Twitter, *Submission 20*, p. 13.

150 Twitter, *Submission 20*, p. 14.

151 Twitter, *Submission 20*, p. 14.

152 Twitter, *Submission 20*, p. 14.

153 Twitter, *Submission 20*, p. 14.

154 Twitter, *Submission 20*, p. 14.

- broadening its definition of harm to 'address content that goes directly against guidance from authoritative sources of global and local public health information';[156] and
- new policies regarding the use of COVID-19 in advertisements.[157]

4.99 Google has likewise increased its removal of COVID-19 misinformation and disinformation, as well as launching a '3 million COVID vaccine counter misinformation fund and 'launch[ing] over 200 new products, with about a $1 billion investment, in countering COVID misinformation'.[158] Mrs Lucinda Longcroft, Google Australia, also confirmed that Google had provided '$5 million worth of free advertising to the Australian government, which has resulted in 20.6 million impressions of authoritative information for Australian users'.[159]

4.100 TikTok reported that it had also undertaken activities in this area:

> …we introduced a global misinformation strategy, which included updates to our policies and rolling out new in-app features to provide more context on COVID-19 and help combat against misleading medical information online. We are working hard to minimise the opportunity for disinformation to gain traction on TikTok, and we are working with public health organisations (like World Health Organisation, International Federation of Red Cross, and popular voices for public health and science, like Bill Nye the Science Guy) to provide trusted information to our community.[160]

4.101 TikTok also confirmed that it removes false medical advice about COVID-19, as well as 'false information that is likely to stoke panic and consequently result in real world harm', conspiracy theories, and hate speech.[161] It also introduced a feature within the application that connects users to authoritative sources of health information.[162]

4.102 WeChat has also prohibited 'content which may constitute a genuine risk of harm or direct threat to public safety'.[163] WeChat noted in its submission, as an

---

155 Twitter, *Submission 20*, p. 14.

156 Twitter, *Submission 20*, p. 14.

157 Twitter, *Submission 20*, pp. 16-17.

158 Mrs Lucinda Longcroft, Google Australia, *Committee Hansard*, 30 July 2021, p. 12.

159 Mrs Lucinda Longcroft, Google Australia, *Committee Hansard*, 30 July 2021, p. 12.

160 TikTok, *Submission 26*, p. 5.

161 TikTok, *Submission 26*, p. 5.

162 TikTok, *Submission 26*, p. 5.

163 WeChat, *Submission 30*, p. 3.

example, that it has prohibited 'the advertising and sale of COVID-19 home testing kits'.[164]

4.103 Facebook has also undertaken activities in this area, including:

- removing misinformation that 'violates our Community Standards and can cause imminent, physical harm';[165]
- reducing the number of people who see content that 'does not violate Community Standards, but still undermines the authenticity and integrity of the platform';[166]
- third-party fact-checking 'to review and rate the accuracy of posts on Facebook and Instagram' and applying warning labels once posts have been identified as false, as well as reducing the distribution of false content;[167]
- displaying prompts to direct users to official sources of information, including from the Australian government and the World Health Organization;[168]
- launching a Coronavirus Information Centre that 'provides a centralised hub of latest updates';[169]
- donating advertising credits to the Australian Federal government and state governments' advertising campaigns;[170]
- introducing a chatbot on WhatsApp to help individual to access the latest information;[171] and
- providing additional context about information they share on COVID-19 via a new notification that appears when people are about to share COVID-19 related links.[172]

4.104 Facebook also removes groups and pages that attempt to spread vaccine misinformation and disinformation, as well as reducing highly forwarded messages until they have been fact-checked.[173] Facebook stated that it is 'rejecting ads and fundraisers that include anti-vaccination misinformation

---

164 WeChat, *Submission 30*, p. 3.

165 Facebook, *Submission 27*, p. 9.

166 Facebook, *Submission 27*, p. 10.

167 Facebook, *Submission 27*, pp. 10-11.

168 Facebook, *Submission 27*, p. 12.

169 Facebook, *Submission 27*, p. 12.

170 Facebook, *Submission 27*, p. 12.

171 Facebook, *Submission 27*, p. 13.

172 Facebook, *Submission 27*, p. 14.

173 Facebook, *Submission 27*, p. 15.

once we find them'.[174] However, Facebook also noted its own limitations in this area:

> Combatting misinformation is a highly challenging and adversarial space, so we still miss things and won't catch everything – but we're making progress.[175]

The Australian government's response to COVID-19 misinformation and disinformation

4.105 The government's response to COVID-19 misinformation and disinformation has developed over time, with more resources and activities being developed as the pandemic progressed throughout late 2020 and early 2021. The Special Broadcasting Service (SBS), since the early stages of the COVID-19 pandemic, has provided news coverage in languages other than English. SBS outlined its activities in this area:

- Comprehensive coverage of reliable health information across all of its 68 language services, including in relation to government issued announcements, quarantine recommendations, evacuations, travel plans, and education advisories;
- Very extensive in language coverage, in particular for Mandarin and Cantonese speaking communities, encompassing community impacts, talk back and interview programs, explainers, dispelling misinformation, and community impacts;
- In addition to the features and interviews, SBS's Mandarin program has also hosted talkback programs, giving listeners the opportunity to speak with public health expert Dr Zhang Ying about any concerns on this issue; and
- As the situation progresses, SBS's extensive coverage has continued to support and service the Persian-speaking and Italian-speaking communities, among others.[176]

4.106 However, as late as 11 December 2020, there was still not a single body dedicated to combatting COVID-19 misinformation and disinformation. Mr Lachlan Colquhoun, Department of the Prime Minister and Cabinet, confirmed that, to his knowledge, there was no COVID-19 disinformation taskforce, stating that he had 'not heard of one'.[177] Mr Neil Hawkins, Acting Deputy Coordinator and Acting First Assistant Secretary, National Counter Foreign Interference Coordination Centre, Department of Home Affairs, stated that

---

[174] Facebook, *Submission 27*, p. 15.

[175] Facebook, *Submission 27*, p. 16.

[176] Special Broadcasting Service, *Submission 6*, p. 3.

[177] Mr Lachlan Colquhoun, First Assistant Secretary, Department of the Prime Minister and Cabinet, *Committee Hansard*, 11 December 2020, p. 2

'there was a COVID taskforce, of which disinformation was a part, but I don't think there was a disinformation taskforce'.[178]

4.107 Dr Richard Johnson, Department of Home Affairs, explained that the Department of Home Affairs has been increasing its activities in relation to disinformation, utilising and expanding on its pre-existing capabilities:

> … we've been working in the online space in the [countering violent extremism] context for a number of years. … During the COVID period, we built up that capability, particularly around the issue of misinformation in the context of the government's handling of the COVID pandemic. We built a cross-agency team which brought in a number of relevant actors—including from the Department of Health … we bolstered our capability, which did involve looking for instances of misinformation online—particularly, but not just, identifying it and then referring it to social media companies for action.[179]

4.108 Dr Johnson further explained that the Department of Home Affairs has also been working with the Department of Health to release fact sheets:

> We did a fact sheet which addressed some of the key themes around misinformation in a COVID context, and we also did a lot of work to publish and translate those materials, noting that Australia is one of the most successful multicultural countries in the world. We set up a kind of translation function to ensure that, in up to 63 languages, we were getting official information out to communities about COVID.[180]

4.109 Additionally, Mr Robert McKinnon, DFAT, also stated that DFAT was undertaking a six-month pilot program, which included a counter disinformation unit.[181] Mr McKinnon confirmed that DFAT had reported on the work of the pilot to the National Security Committee of cabinet, despite the monitoring and framework for the pilot being 'not settled yet':[182]

> We're in the process of establishing a quite detailed monitoring and evaluation framework. That is not settled yet, but, as you would have heard from that hearing, we certainly did have a framework, in terms of our goals and objectives, and we've reported against those goals and objectives.[183]

---

178 Mr Neil Hawkins, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 3.

179 Dr Richard Johnson, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 3.

180 Dr Richard Johnson, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 3.

181 Mr Robert McKinnon, Department of Foreign Affairs and Trade, *Committee Hansard*, 11 December 2020, p. 18.

182 Mr Robert McKinnon, Department of Foreign Affairs and Trade, *Committee Hansard*, 11 December 2020, p. 19.

183 Mr Robert McKinnon, Department of Foreign Affairs and Trade, *Committee Hansard*, 11 December 2020, p. 19.

4.110 By 30 July 2021, the Department of Home Affairs had undertaken further work in this area. Dr Richard Johnson, Department of Home Affairs, described how the Department of Home Affairs' activities had continued on throughout the COVID-19 pandemic:

> We continue to support whole-of-government efforts in the COVID information environment, working very closely with the Department of Health, to put out factual information about the pandemic and to translate that information into up to 63 languages. We also continue to refer instances of misinformation to the social media platforms. Since the start of this year, to the end of June, we have referred 1,735 instances of COVID related misinformation to platforms. We do refer them to the platforms of course. They adjudicate what to do if the particular instance is against their own terms of service.[184]

4.111 Dr Johnson stated that there are 'about seven' full-time equivalent staff within the Department of Home Affairs who are 'identifying and referring instances of COVID related misinformation',[185] and accordingly referring such material to social media platforms for action.[186] Dr Johnson described what kinds of misinformation the staff are seeking to identify:

> We tend to look for misinformation or disinformation in the COVID context under three broad categories. The first is whether, prima facie, it could endanger people's lives—for example, if you were to take X to prevent you from getting Y, where the X in question is something that could be seriously dangerous to an individual's health. There is also information that would seriously compromise the national COVID response. That could come in a range of forms—for example, people putting out disinformation that said, 'Don't get vaccinated, because there's a chip that will link you to 5G networks.' Where we think the COVID environment is being used to vilify members of our community, we would also refer that. Those are the three broad categories that we use in terms of referrals. It is then up to the companies we refer it to to adjudicate it against their own terms of service.[187]

The Joint Committee on Law Enforcement

4.112 The Joint Committee on Law Enforcement released a report in August 2021, entitled *Vaccine related fraud and security risks*. The report ultimately concluded that COVID-19 disinformation and misinformation pose a significant threat:

> It has also become clear that COVID-19 mis/disinformation is not only leading to vaccine hesitancy, a health policy concern, but is also leading to some instances of civil disobedience and protest. COVID-19 mis/disinformation is therefore also a law enforcement issue of growing

184 Dr Richard Johnson, Department of Home Affairs, *Committee Hansard*, 30 July 2021, p. 40.

185 Dr Richard Johnson, Department of Home Affairs, *Committee Hansard*, 30 July 2021, p. 40.

186 Dr Richard Johnson, Department of Home Affairs, *Committee Hansard*, 30 July 2021, p. 40.

187 Dr Richard Johnson, Department of Home Affairs, *Committee Hansard*, 30 July 2021, p. 40.

> concern, particularly as individuals and groups become more radicalised.[188]

4.113 The Joint Committee on Law Enforcement further noted that '[a]ll Australians, law enforcement agencies and governments must work together to ensure that when the pandemic is over, Australia is not left with the infectious disease of disinformation being used for fraudulent purposes, spreading fear and distrust of our necessary institutions'.[189] The report subsequently recommended that:

> …the Department of Home Affairs ensure that the spread of COVID-19 misinformation and disinformation is monitored for extremist content and links to international extremist groups, as well as undertake greater efforts to counter misinformation and disinformation, especially among Aboriginal and Torres Strait Islander communities and culturally and linguistically diverse communities.[190]

[188] Joint Committee on Law Enforcement, *Vaccine related fraud and security risks,* August 2021, p. 34.

[189] Joint Committee on Law Enforcement, *Vaccine related fraud and security risks,* August 2021, p. 34.

[190] Joint Committee on Law Enforcement, *Vaccine related fraud and security risks,* August 2021, p. v.

Chapter 5
Governance

5.1 Various departments across the Australian Government have responsibility for issues associated with foreign interference through social media. This chapter examines the existing legislative framework, including the new voluntary code of practice that applies to some social media platforms. It also assesses the effectiveness of the current departmental arrangements and cooperation activities occurring between social media platforms and government departments, particularly in the context of an upcoming Federal Election.

Relevant legislation

5.2 While several pieces of legislation apply to social media and the online environment more generally, such as those that seek to protect user privacy, and prevent criminal activity online, none specifically address the problem of foreign interference through social media.

5.3 The Department of Home Affairs provided examples of legislation that regulates social media platforms, including:

- *Privacy Act 1988* (Privacy Act), which applies to organisations with an annual turnover of more than $3 million and operating in Australia; this includes organisations such as Facebook, Instagram, Twitter, Snapchat and LinkedIn. The personal information shared on such platforms is protected by the data protection obligations under the Privacy Act.[1]
- *Enhancing Online Safety Act 2015*, which established a two-tiered scheme for the removal of harassing or abusive material from participating social media services allowing tier 1 services to participate on a cooperative basis and requiring tier 2 services to comply on a compulsory basis.[2]
- *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018*, which empowers the eSafety Commissioner to issue removal notices that require the providers of social media services, relevant electronic services, designated internet services and hosting services to take all reasonable steps to support the removal of intimate images, or to cease hosting the image.[3]
- *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, which requires content, internet and hosting providers, including social media platforms, to—within a reasonable time—report to the Australian Federal Police abhorrent violent conduct and remove abhorrent violent

1 Department of Home Affairs, *Submission 16*, p. 9.

2 Department of Home Affairs, *Submission 16*, p. 9.

3 Department of Home Affairs, *Submission 16*, p. 9.

material. The Act also provides the eSafety Commissioner with the power to notify a service provider that abhorrent violent material is available on their service.[4]

5.4 Additionally, the Australian Parliament recently passed the *Online Safety Act 2021* and the *Online Safety (Transitional Provisions and Consequential Amendments) Ac 2021*. These acts retain and replicate certain provisions in the *Enhancing Online Safety Act 2015*, including:

- maintaining the non-consensual sharing of intimate images scheme;
- specifying basic online safety expectations;
- establishing an online content scheme for the removal of certain material; creates a complaints-based removal notice scheme for cyber-abuse being perpetrated against an Australian adult;
- broadening the cyber-bullying scheme to capture harms occurring on services other than social media;
- reducing the timeframe for service providers to respond to a removal notice from the eSafety Commissioner;
- bringing providers of app distribution services and internet search engine services into the remit of the new online content scheme; and
- establishing a power for the eSafety Commissioner to request or require internet service providers to disable access to material depicting, promoting, inciting or instructing in abhorrent violent conduct for time-limited periods in crisis situations.[5]

Australian Code of Practice on Disinformation and Misinformation

5.5 Many social media platforms have adopted a voluntary code of conduct that was produced by the Australian Communications and Media Authority (ACMA) and the industry-led Digital Industry Group (DIGI), a not-for-profit organisation whose members include major social media platforms.

5.6 As noted in Chapter 1, following the Australian Competition and Consumer Commission's Digital platforms inquiry, ACMA was tasked with reporting to government on the adequacy of the platforms' measures and the broader impacts of disinformation by June 2021.[6] This process included ACMA consulting with digital platforms, government and other relevant stakeholders to develop principles and minimum expectations for a voluntary code of conduct.[7]

---

4 Department of Home Affairs, *Submission 16*, p. 9.

5 The Hon. Paul Fletcher MP, Minister for Communications, Urban Infrastructure, Cities and the Arts, *House of Representatives Hansard*, 24 February 2021, p. 1785.

6 Australian Communications and Media Authority (ACMA), *Submission 15*, p. 2.

7 ACMA, *Submission 15*, p. 2.

5.7 A final code of practice for social media platforms was published in February 2021, entitled the Australian Code of Practice on Disinformation and Misinformation. The Code is an opt-in framework for platforms,[8] with Twitter, Google, Facebook, Microsoft, Redbubble, TikTok, Adobe and Apple doing so.[9] The code outlines several guiding principles that platforms ought to abide by, namely:

- protection of freedom of expression;
- protection of user privacy;
- policies and processes concerning advertising placements;
- empowering users;
- integrity and security of services and products; and
- supporting independent researchers.[10]

5.8 Following the adoption of this code, ACMA was required to report to government on a number of matters. These included initial compliance with the code by signatories, the state of disinformation and misinformation on the platforms, and the code's effectiveness in responding to the problems identified by the Australian Competition and Consumer Commission's Digital Platforms Inquiry.[11]

5.9 ACMA provided this report to government in June 2021.[12] However, this report is not publicly available[13] and is currently being considered by the relevant minister.[14] Although ACMA has already reported on the code's functioning over a five-month period,[15] on 30 July 2021 Ms Sullivan stated that

---

8 Digital Industry Group (DIGI), *Australian Code of Practice on Disinformation and Misinformation*, 22 February 2021, p. 3.

9 DIGI, 'Australian Code of Practice on Disinformation and Misinformation', https://digi.org.au/disinformation-code/ (accessed 9 August 2021).

10 DIGI, *Australian Code of Practice on Disinformation and Misinformation*, 22 February 2021, pp. 4-5.

11 ACMA, 'Digital Platforms commit to action on Disinformation', https://www.acma.gov.au/articles/2021-02/digital-platforms-commit-action-disinformation (accessed 9 August 2021).

12 ACMA, 'Online misinformation and news quality in Australia: Position paper to guide code development', https://www.acma.gov.au/australian-voluntary-codes-practice-online-disinformation (accessed 9 August 2021).

13 As at the time of the committee's public hearing on 30 July 2021: see Mr Mike Makin, Assistant Secretary, News and Media Industry Branch, Department of Infrastructure, Transport, Regional Development and Communications, *Committee Hansard*, 30 July 2021, p. 38.

14 Ms Pauline Sullivan, First Assistant Secretary, Online Safety, Media and Platforms Division, Department of Infrastructure, Transport, Regional Development and Communications (DITRDC), *Committee Hansard*, 30 July 2021, p. 38.

15 From its publication in February 2021 to ACMA's reporting date in June 2021.

the code was in its 'early stages' and that 'we need to see how the code works over the forthcoming months'.[16]

Government departments

5.10 Several bodies, strategies or schemes are responsible for addressing issues relating to foreign interference through social media, as well as related misinformation and disinformation. The roles of several departments and strategies in addressing particular elements of foreign interference are described below, as is the role of the cross-departmental Electoral Integrity Assurance Taskforce.

Australian Electoral Commission

5.11 The Australian Electoral Commission (AEC) is responsible for ensuring that Australia has an impartial and independent electoral system. The AEC noted that its practices, and the Australian legislative framework for elections and electoral integrity are 'frequently cited as exemplars of global best practice'.[17] However, it also noted that 'maintaining the highest levels of electoral integrity is a continually evolving challenge'.[18] The AEC further noted that '[t]he broad notion of "integrity" now encompasses cyber security and disinformation, in addition to longer term issues such as physical security and sound operating procedures'.[19]

5.12 The AEC does not monitor electoral communications to ensure that they are accurate, as the *Commonwealth Electoral Act 1918* (the Electoral Act) does not require truth in electoral communication.[20] The AEC noted in its submission that the Electoral Act does require electoral matter to be authorised to provide voters with the source of a communication, which extends to electoral matter that is published on social media.[21]

5.13 In its submission, the AEC outlined measures it took leading into and throughout the 2019 Federal Election campaign, including:

- formalising the Electoral Integrity Assurance Taskforce (EIAT) to address risks to the integrity of the electoral system;
- the 'Stop and Consider' campaign, which encouraged voters to check the source of material they consumed to avoid being misled by potential disinformation;

---

16 Ms Pauline Sullivan, First Assistant Secretary, DITRDC, *Committee Hansard*, 30 July 2021, p. 38.

17 Australian Electoral Commission (AEC), *Submission 14*, p. 1.

18 AEC, *Submission 14*, p. 1.

19 AEC, *Submission 14*, p. 1.

20 AEC, *Submission 14*, p. 1.

21 AEC, *Submission 14*, p. 1.

- engagement with social media organisation and digital platform providers to ensure that the content on these platforms complies with the relevant provisions of the Electoral Act;
- countering electoral disinformation: the AEC monitored social media information online during the election and, where they could, corrected the record as it related to their organisation; the AEC also utilised explanatory infographics and animations to provide key information regarding the election process in an easily consumable format suited to digital media; and
- investigating electoral communications complaints.[22]

5.14 While the AEC does not have a legislative role regarding the truth of electoral communications, it can and does take action on disinformation in relation to the process of administering the election.[23] The AEC noted that, due to the high volume of communications during elections, the AEC 'does not proactively seek out communications that may not comply with the requirements in the Electoral Act, but rather acts on complaints and information provided to us'.[24]

5.15 During the 2019 Federal Election the AEC investigated 528 complaints relating to electoral communications; of these complaints, 109 of these were based on social media content and 28 breaches of the Electoral Act were identified.[25] The AEC stated that 'there were only eleven items of social media communication that resulted in requests by the AEC to the relevant social media company to remove the illegal communication (all of our requests were promptly responded to)'.[26] The AEC stated that it is continuing to build on its relationship with social media organisations.[27]

Counter Foreign Interference Diplomatic Strategy and Counter Foreign Interference Coordinator

5.16 The Counter Foreign Interference Diplomatic Strategy is a pilot program that 'focuses on cooperation with regional partners to enhance their resilience, as well as efforts to build support for stronger international norms against foreign interference'.[28] The strategy is led by the National Counter Foreign Interference Coordinator, which sits within the Department of Home Affairs.[29] The broad

---

22 AEC, *Submission 14*, pp. 1-3.

23 AEC, *Submission 14*, p. 3.

24 AEC, *Submission 14*, p. 3.

25 AEC, *Submission 14*, p. 3.

26 AEC, *Submission 14*, p. 3.

27 AEC, *Submission 14*, p. 4.

28 Department of Foreign Affairs and Trade (DFAT), *Submission 10*, p. 3.

29 DFAT, *Submission 10*, p. 3.

goals of diplomatic action under the Counter Foreign Interference Diplomatic seek to counter foreign interference activity by:

- delivering clear messaging to ensure foreign actors understand what kinds of actions Australia finds unacceptable and that foreign interference is viewed as a core national security concern;
- showing foreign interference actors that their actions can and will be revealed and will generate a meaningful response;
- convincing foreign interference actors that their actions will have costs – and that these costs outweigh the benefits – including through international reputational damage and by underscoring both the strength of Australia's systems and the sophistication of our detection and enforcement capabilities;
- demonstrating that the opportunities for foreign interference are narrowing in Australia and the region, including by increasing regional awareness, reducing vulnerabilities, strengthening institutions; and
- mobilising international collaboration to counter foreign interference and establish globally accepted norms of behaviour.[30]

5.17 Mr Neil Hawkins, Acting Deputy Coordinator and Acting First Assistant Secretary, National Counter Foreign Interference Coordination Centre, Department of Home Affairs, noted that the national Counter Foreign Interference Coordinator's office is 'responsible for coordinating a whole-of-government response to foreign interference'.[31]

5.18 Mr Lachlan Colquhoun, First Assistant Secretary, National Security Division, Department of the Prime Minister and Cabinet, described the Department of Home Affairs as the lead department and the Counter Foreign Interference Coordinator as the lead area for responding to foreign interference through social media:

> The lead agency is the Department of Home Affairs—and all agencies of government are aware of that—through the office of the Counter Foreign Interference Coordinator. All responses to any matter relating to foreign interference, whether it's via social media, via activities within Australia or via activities from offshore, are the responsibility of the Commonwealth Counter Foreign Interference Coordinator.[32]

5.19 Additionally, the National Counter Foreign Interference Coordinator works with the Counter Foreign Interference Taskforce, which sits within the

---

30 Department of Foreign Affairs and Trade, *Submission 10*, p. 3.

31 Mr Neil Hawkins, Acting Deputy Coordinator and Acting First Assistant Secretary, National Counter Foreign Interference Coordination Centre, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 2.

32 Mr Lachlan Colquhoun, First Assistant Secretary, National Security Division, Department of the Prime Minister and Cabinet, *Committee Hansard*, 30 July 2021, p. 22.

Australian Security Intelligence Organisation.[33] The Counter Foreign Interference Taskforce seeks to 'investigate, disrupt and counter' foreign interference.[34]

International Cyber Engagement Strategy

5.20 The Department of Foreign Affairs and Trade leads the implementation of Australia's International Cyber Engagement Strategy (ICES). Released in October 2017, the ICES seeks to 'maintain an open, free and secure cyberspace that drives economic growth, protects national security and fosters international stability'.[35]

5.21 The ICES has seven key themes, which are to:

- maximise opportunities for economic growth and prosperity through digital trade;
- foster good cyber security practices;
- reduce the risk of cybercrime;
- promote peace and stability in cyberspace;
- advocate for multi-stakeholder Internet governance;
- promote respect for human rights and democratic principles online; and
- encourage the use of digital technologies to achieve sustainable development.[36]

Foreign Influence Transparency Scheme

5.22 The *Foreign Influence Transparency Scheme Act 2018* created the Foreign Influence Transparency Scheme, which came into effect on 10 December 2018.[37] The Attorney-General's Department has ownership of the scheme. Under the scheme, a person is required to publicly register with if they undertake a 'registrable activity' in Australia for the purpose of political or governmental influence on behalf of a foreign principal. A registrable activity can be:

- general political lobbying;
- parliamentary lobbying;
- communications activity; or
- disbursement activity.[38]

---

33 Mr Neil Hawkins, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 7.

34 Mr Neil Hawkins, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 7.

35 DFAT, *Submission 10*, p. 4.

36 DFAT, *Submission 10*, p. 5.

37 Attorney-General's Department, *Submission 13*, p. 4.

38 Attorney-General's Department, *Submission 13*, p. 8.

5.23 Foreign principals can be 'foreign governments, foreign political organisations, foreign government related entities, and foreign government related individuals'.[39]

5.24 Significantly, this scheme is designed to address foreign influence—an entirely legal activity, which is regularly undertaken by many governments—as opposed to foreign interference.[40] The Attorney-General's Department noted that such influence activities 'when conducted in an open and transparent manner, are a normal aspect of international relations and diplomacy and can contribute positively to public debate'.[41]

5.25 During election periods, the Foreign Influence Transparency Scheme imposes additional obligations. From the day that the writs are issued to when the last polling stations close on voting day, activities must be lodged with the Attorney-General's Department within seven days rather than the usual 14. Following this, the Department must publicly publish those activities within 48 hours, rather than within the normal prescribed time of four weeks.[42]

5.26 During the 2019 Federal Election, the Attorney-General's Department received referrals from the Electoral Integrity Assurance Taskforce to 'consider whether any registrable activities were being undertaken, and whether the posts on social media needed to be registered and contain the appropriate disclosures'.[43] The Attorney-General's Department described the difficulties in assessing the referral of such posts:

> In making a determination about whether registration obligations would apply, there were a number of factors the department needed to take into consideration – some of which were difficult to establish with a strong degree of certainty. In particular, the number of social media posts and different platforms used in the federal election to share information and opinions on candidates was significant and it was often not clear whether the posts were on behalf of a foreign actor.[44]

5.27 The Attorney-General's Department further stated that, despite these difficulties, where material was identified that may not have complied with the *Foreign Influence Transparency Act 2018*, the department 'engaged with government counterparts and, where appropriate, social media companies to

---

39 Attorney-General's Department, *Submission 13*, p. 8.

40 Attorney-General's Department, *Submission 13*, p. 8.

41 Attorney-General's Department, *Submission 13*, p. 8.

42 Attorney-General's Department, *Submission 13*, p .9.

43 Attorney-General's Department, *Submission 13*, p. 9.

44 Attorney-General's Department, *Submission 13*, p. 9.

work cooperatively to assess whether the obligations under scheme applied to the material'.[45]

Electoral Integrity Assurance Taskforce

5.28 The Electoral Integrity Assurance Taskforce (EIAT) is a cross-departmental taskforce. Prior to the 2018 by-elections and 2019 Federal Election, the EIAT was formed to 'address risks to the integrity of the electoral system'.[46] The AEC stated that the taskforce 'comprised a range of Commonwealth agencies who were co-located during the federal election and provided timely guidance and expertise to the AEC on a broad range of integrity issues, including cyber security and disinformation'.[47] Member agencies of the EIAT include:

- Australian Electoral Commission;
- Department of Finance;
- Department of Prime Minister and Cabinet;
- Department of Infrastructure, Transport, Regional Development and Communications;
- Attorney-General's Department;
- Department of Home Affairs; and
- Australian Federal Police.

5.29 The EIAT is also supported by intelligence agencies where required,[48] including the Office of National Intelligence, the Australian Signals Directorate and the Australian Security Intelligence Organisation.[49] The EIAT is also overseen by an oversight board, which comprises the same members as the EIAT itself.[50]

5.30 The EIAT is also supported by the Electoral Integrity Intelligence Forum, which Mr Patrick Hallinan, Acting First Assistant Secretary, Counter Foreign Interference Coordination Centre, Department of Home Affairs, described as a body chaired by the Counter Foreign Interference Coordination Centre, comprised of representatives from the national security community, that 'provide[s] coordinated support and advice to the EIAT board and, through

---

45 Attorney-General's Department, *Submission 1*3, pp. 9-10.

46 AEC, *Submission 14*, p. 2; and Department of Home Affairs, *Submission 16*, p. 6.

47 AEC, *Submission 14*, p. 2.

48 AEC, 'Electoral Integrity Assurance Taskforce', https://www.aec.gov.au/elections/electoral-advertising/electoral-integrity.htm (accessed 14 August 2021).

49 Department of Home Affairs, *Submission 16*, p. 6.

50 Mr Lachlan Colquhoun, Department of the Prime Minister and Cabinet, *Committee Hansard*, 30 July 2021, p. 19.

the board, to the commissioner on any national security concerns from an intelligence perspective'.[51]

Mandate and terms of reference

5.31 Despite the EIAT being established in 2018, the EIAT has not received a formal mandate by government. Mr Lachlan Colquhoun, Department of the Prime Minister and Cabinet, described to the committee how, the establishment of the EIAT was 'almost organic' and that it was not established with a set mandate.[52] In response to a request refer to a document that outlined the EIAT's role, Mr Colquhoun stated that one did not exist 'at this point' and that 'there is some work underway within government to consider how to more concretely codify the role of the task force'.[53] Mr Colquhoun further stated:

> The Australian Electoral Commission has started preparing a paper, basically formalising the task force and making sure that there's a common understanding of its role and remit, but that paper doesn't have any status at this point, and I wouldn't want to go too much further given it has not been put to government formally yet.[54]

5.32 While no mandate for the EIAT's activities exists, the EIAT operate under a terms of reference, which were endorsed by the oversight board in April 2021.[55] However, this document is regarded as classified material. Mr Jeff Pope, Deputy Electoral Commissioner, ACE, stated:

> We do have terms of reference, but it is a classified document and, therefore, we've been limited in our ability to be able to share that more broadly.[56]

5.33 When asked if the terms of reference would be made public, Mr Tom Rogers, AEC, stated:

> We will be releasing information about the activities of the task force, yes.[57]

5.34 Mr Tom Rogers, AEC, confirmed that the EIAT's primary role is as an information sharing forum, which also existed to provide advice to the

---

51 Mr Patrick Hallinan, Acting First Assistant Secretary, Counter Foreign Interference Coordination Centre, Department of Home Affairs, Committee Hansard, 30 July 2021, p. 41.

52 Mr Lachlan Colquhoun, Department of the Prime Minister and Cabinet, *Committee Hansard*, 30 July 2021, p. 20.

53 Mr Lachlan Colquhoun, Department of the Prime Minister and Cabinet, *Committee Hansard*, 30 July 2021, p. 20.

54 Mr Lachlan Colquhoun, Department of the Prime Minister and Cabinet, *Committee Hansard*, 30 July 2021, p. 20.

55 Attorney-General's Department, *Questions on Notice*, *Answers to questions on notice* (30 July 2021 public hearing; received 13 August 2021), p. 1.

56 Mr Jeff Pope, Deputy Electoral Commissioner, AEC, *Committee Hansard*, 30 July 2021, p. 25.

57 Mr Tom Rogers, AEC, *Committee Hansard*, 30 July 2021, p. 25.

Electoral Commissioner.[58] Mr Jeff Pope, AEC, expanded on the role of the EIAT:

> Essentially, the role of the task force is for all of the agencies, within their legislative roles and functions, to collaborate and assess information and referrals that might be referred into the task force or that they may detect in their own right; to determine whether there are any matters that may impact on the potential integrity of election processes and election results; and to provide advice to the Electoral Commissioner with respect to those matters.[59]

5.35 Mr Patrick Hallinan, Department of Home Affairs, described the broadness of the EIAT's remit regarding electoral integrity:

> The EIAT focuses on a number of things. It focuses on, obviously, electoral integrity related matters more generally, but, to step that out for you, foreign interference is one of the elements of electoral integrity that the EIAT is concerned with, but it's also concerned with things to do with physical security, whether that's terrorism or process related activity. It's also concerned with things to do with cybersecurity. I think it's attempting to bring a broader consideration of the full range of activities which may impede the conduct of an election or otherwise affect the conduct of an election and provide that support primarily to the Electoral Commissioner.[60]

5.36 Mr Tom Rogers, AEC, noted that the EIAT is not 'empowered to make decisions' regarding public communications.[61] Mr Rogers further stated that '[t]he task force would be a focus of discussion where agency heads that are represented by those on the task force would then make those decisions'.[62] Mr Rogers confirmed that the EIAT does not have any further decision-making capacity, rather that it is primarily an information sharing forum that also provides advice to the Electoral Commissioner.[63]

5.37 When asked about the EIAT's ability to brief members of cabinet, Mr Nathan Williamson, Deputy Secretary, Governance and Resource Management, Department of Finance, also confirmed that the EIAT itself did not have ability to brief members of cabinet, rather that individual departments would do so in line with their usual responsibilities.[64]

---

58 Mr Tom Rogers, AEC, *Committee Hansard*, 30 July 2021, p. 28.

59 Mr Jeff Pope, AEC, *Committee Hansard*, 30 July 2021, p. 25.

60 Mr Patrick Hallinan, Department of Home Affairs, *Committee Hansard*, 30 July 2021, p. 42.

61 Mr Tom Rogers, AEC, *Committee Hansard*, 30 July 2021, p. 25.

62 Mr Tom Rogers, AEC, *Committee Hansard*, 30 July 2021, p. 25.

63 Mr Tom Rogers, AEC, *Committee Hansard*, 30 July 2021, p. 28.

64 Mr Nathan Williamson, Deputy Secretary, Governance and Resource Management, Department of Finance, *Committee Hansard*, 30 July 2021, p. 28.

5.38 Additionally, should the EIAT become aware of an instance of foreign interference in an Australian election, the information would be referred to the Electoral Commissioner. Mr Patrick Hallinan, Department of Home Affairs, described how this process would occur:

> I would expect that, were there to be an instance of a deliberate targeted campaign which constituted foreign interference in an electoral context, that matter would be raised with the Electoral Integrity Assurance Taskforce construct in the first instance, and that that advice would be provided to the Electoral Commissioner, and the Electoral Commissioner would be free to do whatever they so determined to do in respect of that. More generally, agencies who comprise the Electoral Integrity Assurance Taskforce construct would no doubt be providing advice within their chains as appropriate, whether it was to ministers in accordance with the caretaker conventions or at their own initiative under their statutory responsibilities.[65]

Preparations for the upcoming Federal Election

5.39 Officials provided evidence to the committee asserting that the role of the EIAT will increase in importance as the next Federal Election draws nearer. In preparation for the next Federal Election, Mr Peter Rush, Assistant Secretary, Parliamentary and Government Branch, Department of the Prime Minister and Cabinet, stated that the EIAT has been 'increasing its tempo' since March 2021:

> Since about March this year the task force has been increasing its tempo to be prepared for the next federal election. The board has been meeting a little bit more regularly and the task force has also been getting together on a more regular basis. They've started consulting online media platforms to discuss the processes that will be in place during the electoral process.[66]

5.40 Further to this, Mr Lachlan Colquhoun, Department of the Prime Minister and Cabinet, noted that the role of the EIAT is limited between election cycles:

> … the task force is a bit of a virtual task force. All the people who participate have day jobs. In between election cycles their involvement will be very small, and it will ramp up to being almost full-time in the lead-up to an election.[67]

5.41 Regarding the upcoming Federal Election, Mr Tom Rogers, AEC, stated that the EIAT would be co-located in the AEC's Command Centre, which 'is currently being constructed following the budget initiative in October last

---

65 Mr Patrick Hallinan, Department of Home Affairs, *Committee Hansard*, 30 July 2021, p. 42

66 Mr Peter Rush, Department of the Prime Minister and Cabinet, *Committee Hansard*, 30 July 2021, p. 20.

67 Mr Lachlan Colquhoun, Department of the Prime Minister and Cabinet, *Committee Hansard*, 30 July 2021, p. 19.

year'.[68] Mr Rogers also noted that the EIAT has started meeting with social media platforms in preparation for the Federal Election.[69]

Cooperation between social media platforms and government

5.42 Social media platforms reported to the committee that they had interactions with various government departments and bodies. Given that social media platforms are currently the arbiters of what content remains on their platforms, government engagement with cooperative social media platforms is critical. This section describes the types of interactions that various social media platforms have with Australian government departments.

5.43 Facebook submitted that it had been working with Australian electoral authorities and that, prior to the 2019 Federal Election, it had 'established a productive working relationship with members of the Government's election integrity taskforce'[70] and noted that it 'worked closely to quickly respond to all issues raised with us by Australian Government agencies'.[71]

5.44 Facebook added that it also works with state and territory electoral commissions to 'establish similar referral arrangements before elections in their states and territories'.[72] At the committee's public hearing, Facebook also reported that it had been receiving referrals from multiple parts of the Australian government regarding inappropriate content, including the Department of Home Affairs, Department of Health, and DFAT.[73]

5.45 TikTok noted its work with the Australian Communications and Media Authority.[74] In giving evidence to the committee, the Department of Home Affairs also noted that TikTok had provided assistance in 'a particular exercise that [the Department of Home Affairs] ran on the vector of online harmful content in terms of a terrorist incident'.[75]

5.46 WeChat described how it has been engaged in ongoing, cooperative relationships with Australian government agencies, including the Department

---

68 Mr Tom Rogers, AEC, *Committee Hansard*, 30 July 2021, p. 24.

69 Mr Tom Rogers, AEC, *Committee Hansard*, 30 July 2021, p. 24.

70 Facebook, *Submission 27*, p. 19. The organisations Facebook states that it worked with are the AEC, the National Counter Foreign Interference Coordinator, the Department of Home Affairs, and the Department of Communications and the Arts (now DITRDC).

71 Facebook, *Submission 27*, p. 19.

72 Facebook, *Submission 27*, p. 19.

73 Mr Josh Machin, Head of Policy, Australia, Facebook, *Committee Hansard*, 30 July 2021, p. 5.

74 TikTok, *Submission 26*, p. 4.

75 Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy Division, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 16.

of Home Affairs, the Australian Electoral Commission, and the Attorney-General's Department.[76]

5.47 Google stated that it works with Australia's law enforcement and intelligence community, including the National Counter Foreign Interference Coordinator.[77] Mrs Lucinda Longcroft noted the wide variety of agencies that Google was working with, which included the Australian Federal Police, eSafety Commissioner, the Australian Competition and Consumer Commission, Australian Securities and Investments Commission, the Australian Taxation Office, and ACMA.[78]

5.48 Twitter has previously worked with the AEC, DFAT and Department of Home Affairs, as well as the EIAT. Ms Kara Hinesley, Director of Public Policy, Australia and New Zealand, Twitter, noted that Twitter worked with the EIAT during the 2019 Federal Election and has already begun 'facilitating conversations and meetings' ahead of the upcoming Federal Election.[79]

5.49 Government departments do occasionally contact Google to request the removal of content. However, Google noted that, while government departments do occasionally flag content with the company for removal, the vast majority of its content is self-identified, with only 86 of the 9.6 million videos removed by Google being flagged by the Australian Government.[80]

5.50 Government departments likewise described their interactions with social media platforms. The AEC noted that it has established and maintained ongoing relationships with prominent social media and digital platform providers in order to ensure the content on these platforms complies with the relevant provisions of the Electoral Act.[81] The AEC described how its level of engagement with the social media platforms increased in the lead-up to the last Federal Election:

> The level of engagement with these organisations was both vastly increased and improved for the 2019 federal election when compared to previous electoral events. We engaged, in person, with Facebook, Twitter, Google and WeChat in relation to the 2019 federal election in order to better understand their platforms, any relevant initiatives (e.g. political advertising transparency libraries), their policies and establish procedures

---

76 WeChat, *Submission 30*, p. 3.

77 Mr Richard Salgado, Director, Law Enforcement and Information Security, Google, *Committee Hansard*, 30 July 2021, p. 11 and p. 13.

78 Mrs Lucinda Longcroft, Director, Government Affairs and Public Policy, Australia and New Zealand, Google Australia, *Committee Hansard*, 30 July 2021, p. 13.

79 Ms Kara Hinesley, Director of Public Policy, Australia and New Zealand, Twitter, Committee Hansard, 30 July 2021, p. 49.

80 Mrs Lucinda Longcroft, Google Australia, *Committee Hansard*, 30 July 2021, p. 11.

81 AEC, *Submission 14*, p. 3.

> to address electoral communications that breached electoral laws (e.g. was not properly authorised).[82]

5.51 Mr Tom Rogers, AEC, described how the EIAT is engaging with social media platforms prior to the next Federal Election:

> One of the most relevant planning activities has included proactive meetings with prominent social media companies. These meetings provide an opportunity to re-establish key contact points and procedures to ensure we can respond quickly to address any issues that may emerge at election time.[83]

5.52 The relationship between social media platforms and governments is not always an easy one. Dr Richard Johnson, First Assistant Secretary, Social Cohesion, Department of Home Affairs, reported how the department had run into difficulties when attempting to report extremist content to social media platforms:

> Some of the platforms … do not have a referral mechanism at all. Some of the offshore platforms which have built an ethos around freedom of expression et cetera, will not have a referral mechanism, so we can't refer it to them.[84]

5.53 There have also been historic difficulties with the AEC's attempt to engage with social media platforms. The Law Council of Australia also highlighted reports that challenges have arisen for the AEC when attempting to counter unauthorised online advertising that originates from overseas.[85] In providing an example, the Law Council of Australia outlined Facebook's previous non-compliance with Australia's domestic advertising laws. It was reported in 2019 that Facebook had not adequately applied the rules set out by the Electoral Act to paid political advertising on its platform and did not respond to AEC inquiries about the source of advertising in a timely manner.[86]

5.54 Additionally, there is confusion from the social media platforms' perspective regarding reporting requirements (or lack thereof) to the Australian government. Following questioning regarding reporting arrangements, Mr Lee Hunter, General Manager, TikTok Australia and New Zealand, noted that—should TikTok find evidence of foreign interference on its platform—it was not aware of any requirement to report it, although he noted TikTok would

---

82 AEC, *Submission 14*, p. 3.

83 Mr Tom Rogers, AEC, *Committee Hansard*, 30 July 2021, p. 24.

84 Dr Richard Johnson, First Assistant Secretary, Social Cohesion, Department of Home Affairs, *Committee Hansard*, 30 July 2021, pp. 43-44.

85 Law Council of Australia, *Submission 18*, p. 33.

86 Law Council of Australia, *Submission 18*, p. 32.

voluntarily provide this information.[87] Further to this, it was not clear which department ought to be reported to.[88]

5.55 Mr Neil Hawkins, Department of Home Affairs, when asked which department social media platforms would report CIB from a foreign state actor to, stated:

> I'm not aware. I don't think they would talk to us [Department of Home Affairs]. They may talk to the Australian Cyber Security Centre, but I couldn't answer that point.[89]

5.56 When asked if platforms ought to report such content to DFAT, Mr Robert Hawkins, Assistant Secretary, DFAT, said that the department would 'welcome that' but noted that '[w]e have engagements with them, but it's not necessarily on, for example, an alert reporting basis.[90]

5.57 When asked about TikTok's statement regarding a lack of a clear reporting mechanism, Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy Division, Department of Home Affairs, stated that:

> …it depends on the particular threat. If it's an image based abuse complaint or a particular issue on their platform, Cyber Report, through the eSafety Commissioner, is the reporting mechanism. If it's a cybersecurity incident, it's ReportCyber, through the partnership of the Australian Cyber Security Centre. There are obviously reporting mechanisms available through business liaison with the Australian Security Intelligence Organisation. So it really depends on the particular threat.[91]

5.58 In response to a follow-up question, which asked if any department was 'providing cogent guidance to the platforms about what their obligations are and what the appropriate communication channels are', Mr Hansford stated:

> I think the answer is that there are a range of different places within government. There is no single place where social media companies can go to get comprehensive, whole-of-nation advice about each of the different vectors.[92]

5.59 Aside from this lack of a singular reporting mechanism, some social media platforms have specifically requested further cooperation with government in

---

87 Mr Lee Hunter, General Manager, TikTok Australia and New Zealand, TikTok Australia, *Committee Hansard*, 25 September 2020, p. 11.

88 Mr Lee Hunter, TikTok Australia and New Zealand, TikTok Australia, and Mr Brent Thomas, Director of Public Policy, Australia and New Zealand, TikTok Australia *Committee Hansard*, 25 September 2020, pp. 11-12.

89 Mr Neil Hawkins, Department of Home Affairs, C*ommittee Hansard*, 11 December 2020, p. 5.

90 Mr Robert Hawkins, Assistant Secretary, DFAT, C*ommittee Hansard*, 11 December 2020, p. 6.

91 Mr Hamish Hansford, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 17.

92 Mr Hamish Hansford, Department of Home Affairs, *Committee Hansard*, 11 December 2020, p. 17.

other areas. Facebook submitted that it 'believe[s] there are greater steps the Australian Government could take to engage in information-sharing with digital platforms and industry more broadly about foreign interference or influence operations'.[93] Facebook added that it also works with state and territory electoral commissions to 'establish similar referral arrangements before elections in their states and territories'.[94]

5.60 Ms Kara Hinesley, Twitter, likewise raised the importance of further cooperation between governments and social media platforms:

> What is important is to approach the issue as a broad geopolitical challenge, not one of content moderation. Removal of content alone will not address this challenge. The threat we face requires extensive partnership and collaboration with government entities, civil society, experts and industry peers. We each possess information that others do not have, and our combined efforts are more powerful together in combating these threats.[95]

Senator Jenny McAllister
Chair
Labor Senator for New South Wales

[93] Facebook, *Submission 27*, p. 20.

[94] Facebook, *Submission 27*, p. 19.

[95] Ms Kara Hinesley, Twitter, *Committee Hansard*, 30 July 2021, pp. 47-48.

Senator Jim Molan's additional comments

1.1 I acknowledge the work of the committee in undertaking this important inquiry, and thank the witnesses who have participated in giving evidence.

1.2 Though I agree with parts of the majority report, I will be providing more fulsome additional comments in the new year to address concerns I have with some of the recommendations and evidence provided to the committee.

Senator Jim Molan AO DSC
Deputy Chair
Liberal Senator for New South Wales

Submissions and additional information

1 RAND Australia
2 Dr Jake Wallis and Mr Thomas Uren (Australian Strategic Policy Institute)
3 Mr Robert Size
4 China Policy Centre
5 Ms Melissa Harrison
6 Special Broadcasting Service Corporation (SBS)
7 Dr Bruce Arnold and Dr Benedict Sheehy
8 News and Media Research Centre (University of Canberra)
9 Australian Citizens Party
10 Department of Foreign Affairs and Trade
11 Law Society of New South Wales: Young Lawyers
- 11.1 Supplementary to submission 11

12 Osmond Chiu and Kun Huang
13 Attorney-General's Department
14 Australian Electoral Commission
15 Australian Communications and Media Authority
16 Department of Home Affairs
17 Responsible Technology Australia
18 Law Council of Australia
19 Allens Hub for Technology, Law and Innovation; the Datafication and Automation of Human Life; and the Society on Social Implications of Technology
20 Twitter
- 20.1 Supplementary to submission 20

21 Dr Carlo Kopp
22 Ms Joy Bell
23 Google Australia
24 Australian Muslim Advocacy Network
- 24.1 Confidential
- 24.2 Confidential

25 Principle Co
26 TikTok Australia
27 Facebook
- 27.1 Supplementary to submission 27

28 Paul Dabrowa
29 Mr Tom Sear
- 29.1 Supplementary to submission 29
- Attachment 1
- Attachment 2

30 WeChat International Pte Ltd
31 Australia Institute
- 31.1 Supplementary to submission 31
- 31.2 Supplementary to submission 31
- 31.3 Supplementary to submission 31

32 *Confidential*
33 *Confidential*
34 Mr John Xu
35 The Council on Middle East Relations
36 Engineers Australia
37 UNSW Law Society
38 Australian National University Law Reform and Social Justice Research Hub
39 Mr Benjamin Cronshaw
40 John Abdelmalek, Kyron Johnson, Michael Barberio, and Mathew Bubica, with Dr James Scheibner
41 Australasian Cyber Law Institute
42 Dr Shumi Akhtar
43 Migration Council Australia and Centre for Digital Wellbeing

Additional Information

1 'The Weaponization of Information: The Need for Cognitive Security': Dr Rand Waltzman's written testimony to a US Senate Armed Services Committee hearing on 27 April 2017 ('Cyber Enabled Influence Operations').
2 Joint Standing Committee on Electoral Matters, 'Interim report on all aspects of the conduct of the 2019 Federal Election and matters related thereto: Delegation to the International Grand Committee, Dublin, Ireland', 15 May 2020

Answer to Question on Notice

1 Answers to questions on notice - TikTok Australia - Canberra (25 September 2020 public hearing) - received 25 October 2020
2 Answers to written questions on notice - Department of Home Affairs (issued on 23 October 2020) - received 6 November 2020
3 Answer to questions on notice - Department of Foreign Affairs and Trade - Canberra (11 December 2020 public hearing) - received 10 March 2021 (M&C Saatchi)
4 Answer to questions on notice - Department of Foreign Affairs and Trade - Canberra (11 December 2020 public hearing) - received 10 March 2021 (disinformation related activities)
5 Answers to written questions on notice - Department of Prime Minister and Cabinet (issued on 23 October 2020) -received 29 July 2021
6 Answers to questions on notice - Department of Prime Minister and Cabinet - Canberra (11 December 2020 public hearing) - received 29 July 2021

7 Answers to questions on notice - Department of Infrastructure, Transport, Regional Development and Communications - Canberra (30 July 2021 public hearing) - received 10 August 2021
8 Answers to questions on notice - Attorney-General's Department - Canberra (30 July 2021 public hearing) - received 13 August 2021
9 Answers to questions on notice - Department of Home Affairs - Canberra (30 July 2021 public hearing) - received 13 August 2021
10 Answer to question on notice - Department of Infrastructure, Transport, Regional Development and Communications - Canberra (30 July 2021 public hearing) - received 19 August 2021
11 Answers to questions on notice - Twitter - Canberra (30 July 2021 public hearing) - received 20 August 2021
12 Answers to questions on notice - Facebook - Canberra (30 July 2021 public hearing) - received 12 November 2021

Media Releases

1 Media Release - Opening of Submissions
2 Media Release - Upcoming Public Hearings in 2020
3 Media Release - Public Hearing of 25 September 2020
4 Media Release - Reopening of Submissions

Public hearings and witnesses

Monday, 22 June 2020
2S1 and via videoconference

Berkman Klein Centre for Internet & Society
- Ms evelyn douek

Stanford Internet Observatory
- Mr Alex Stamos

Australian Strategic Policy Institute
- Dr Jake Wallis, Senior Analyst
- Mr Thomas Uren

National Security College, ANU
- Ms Katherine Mansted

University of Canberra
- Dr Mathieu O'Neil
- Professor Robert Ackland
- Dr Michael Jansen

Monash University
- Dr Carlo Kopp

Friday, 25 September 2020
2S3 and via videoconference

University of Canberra's News and Media Research Centre
- Dr Michael Jensen
- Professor Kerry McCallum
- Associate Professor Mathieu O'Neil

TikTok Australia
- Mr Brent Thomas, Director of Public Policy
- Mr Lee Hunter, General Manager
- Mr Roland Cloutier, Chief Security Officer

Friday, 11 December 2020
Committee Room 2S3, Parliament House
Canberra ACT

Attorney-General's Department
- Ms Sarah Chidgey, Deputy Secretary, Integrity and International Group

Department of Foreign Affairs and Trade

- Mr Robert McKinnon, Acting First Assistant Secretary, International Security Division
- Dr Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology

Department of Home Affairs

- Mr Neil Hawkins, Acting Deputy National Counter Foreign Interference Coordinator
- Mr Hamish Hansford, First Assistant Secretary Cyber, Digital and Technology Policy
- Dr Richard Johnson, First Assistant Secretary, Social Cohesion Division

Department of Prime Minister and Cabinet

- Mr Lachlan Colquhoun, First Assistant Secretary, National Security
- Ms Celeste Moran, First Assistant Secretary, Government
- Mr Peter Rush, Parliamentary and Government

Friday, 30 July 2021

Committee Room 2S3
Parliament House
CANBERRA ACT and via videoconference

Facebook

- Mr Nathaniel Gleicher, Global Head of Security Policy
- Mr Josh Machin, Head of Public Policy, Australia

Google Australia

- Mr Richard Salgado, Director, Law Enforcement and Information Security
- Ms Lucinda Longcroft, Director, Government Affairs and Public Policy, Australia and New Zealand

Department of Prime Minister and Cabinet

- Mr John Reid, First Assistant Secretary, Government Division
- Mr Lachlan Colquohoun, First Assistant Secretary, National Security Division
- Mr Peter Rush, Assistant Secretary, Parliamentary and Government

Australian Electoral Commission

- Mr Tom Rogers, Electoral Commissioner
- Mr Jeff Pope APM, Deputy Electoral Commissioner

Department of Finance

- Mr Scott Dilley, First Assistant Secretary, Governance, Governance and Resource Management

- Mr Nathan Williamson, Deputy Secretary, Governance and Resource Management

Department of Infrastructure, Transport, Regional Development and Communications

- Mr Mike Makin, Assistant Secretary
- Ms Pauline Sullivan, First Assistant Secretary
- Ms Bridget Gannon, First Assistant Secretary, Digital Platforms and Online Safety Branch

Attorney-General's Department

- Ms Autumn Field, Assistant Secretary, Transparency and Criminal Law Branch
- Ms Julia Galluccio, Assistant Secretary, Information Law Branch

Department of Home Affairs

- Dr Richard Johnson, First Assistant Secretary Social Cohesion
- Mr Hamish Hansford, First Assistant Secretary, Cyber, Digital and Technology Policy
- Mr Patrick Hallinan, Acting First Assistant Secretary, Counter Foreign Interference Coordination Centre

Twitter

- Ms Kathleen Reen, Director of Public Policy, Australia and New Zealand
- Ms Kara Hinesley, Director of Public Policy, Australia and New Zealand