

The Senate

Select Committee on Foreign
Interference through Social Media

Senate Select Committee on Foreign
Interference through Social Media

August 2023

© Commonwealth of Australia 2023

ISBN 978-1-76093-525-2 (Printed version)

ISBN 978-1-76093-525-2 (HTML version)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International License.



The details of this licence are available on the Creative Commons website:

<https://creativecommons.org/licenses/by-nc-nd/4.0/>.

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

Contents

Members	v
Abbreviations and acronyms.....	vii
Foreword.....	xi
List of recommendations	xv
Chapter 1—Introduction and background	1
Definitions.....	2
What is foreign interference	4
Foreign interference via social media.....	5
Chapter 2—Foreign interference in Australia	9
Foreign interference in Australia	9
Tactics	22
Emerging Tactics.....	26
Chapter 3—International issues.....	31
Europe.....	31
United States	41
United Kingdom	43
Canada.....	44
New Zealand	45
Pacific region	46
International digital literacy campaigns.....	47
Chapter 4—Government: Current practice	51
Current legislative settings	51
Government counter-interference entities.....	54
Recent policy responses and initiatives	62
Chapter 5—Government: ideas for action.....	69
Lead agency	70
Standards-based regulation	71
Legal remedies.....	76
Countermeasures	81
Cross-sector collaboration.....	84

Chapter 6—Platforms—Current practice and identified gaps	87
Platform responsibilities	87
Platform actions to address interference	88
Ongoing concerns	92
Platforms and authoritarian states	106
Chapter 7—Building the capacity of civil society.....	125
A role for civil society organisations, expert centres and researchers.....	125
Building resilience through public education.....	128
Mainstream media	137
Diaspora communities	138
Chapter 8—Committee view and recommendations	143
Overall committee view	143
Platform transparency	145
Platforms headquartered in authoritarian states	150
Building the capacity of government.....	157
Intelligence briefings	161
Building the capacity of civil society.....	162
Protecting our neighbours	167
Additional comments from Government Senators	169
Australian Greens' Additional Comments.....	173
Appendix 1—Submissions, tabled documents and additional information.....	175
Appendix 2—Public hearings and witnesses	179
Appendix 3—46th Parliament inquiry recommendations	183

Members

Chair

Senator James Paterson

LP, VIC

Deputy Chair

Senator Jess Walsh

ALP, VIC

Members

Senator Claire Chandler

LP, TAS

Senator Raff Ciccone

ALP, VIC

Senator Sarah Hanson-Young

AG, SA

Secretariat

Ms Apolline Kohen, Committee Secretary

Dr Sean Turner, Committee Secretary

Ms Kate Gauthier, Principal Research Officer

Ms Monique Nielsen, Senior Research Officer

Ms Georgia O'Connor, Administrative Officer

Ms Ella Shea, Administrative Officer

Ms Stacey Sullivan, Administrative Officer

Po Box 6100

Email: foreigninterference47.sen@aph.gov.au

Parliament House

Canberra ACT 2600

Abbreviations and acronyms

5D	dismiss, distort, distract, dismay, divide objectives
AAP	Australian Associated Press
ABCDE framework	actors, behaviours, content, degree, and effect framework
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ACRI	Australia-China Relations Institute, University of Technology Sydney
ACSC	Australian Cyber Security Centre
ADM	automated decision making
AEC	Australian Electoral Commission
AFP	Australian Federal Police
AFP	Agence France-Presse
AGD	Attorney-General's Department
AHRC	Australian Human Rights Commission
AI	artificial intelligence
Allens Hub Joint Submission	University of New South Wales Allens Hub for Technology Law and Innovation, Deakin University Centre for Cyber Security Research and Innovation and Institute of Electrical and Electronics Engineers Society on Social Implications of Technology
API	application programming interface
ASD	Australian Signals Directorate
ASEAN	Association of Southeast Asian Nations
ASIO	Australian Security Intelligence Organisation
ASPI	Australian Strategic Policy Institute
bots	robots or algorithmically-driven computer programs designed to carry out specific tasks online, for example, mimicking the behaviour of real users
CALD	culturally and linguistically diverse
CCP	Chinese Communist Party
CFI	counter foreign interference
CIB	co-ordinated inauthentic behaviour
CISA	Cybersecurity and Infrastructure Security Agency (US)
CISC	Cyber and Infrastructure Security Centre
CLO	Community Liaison Officer
COO	Chief Operating Officer
Criminal Code	<i>Criminal Code Act 1995</i>
CSIS	Canadian Security Intelligence Service
CSO/s	Civil Society Organisation/s

DC	District of Columbia (Washington, DC, US)
Defence and Security Institute	Defence and Security Institute, University of Adelaide
Department of Communications	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
DIGI	Digital Industry Group Inc
DIGI Code	<i>Australian Code of Practice on Misinformation and Disinformation</i>
DISARM framework	Disinformation Analysis and Risk Management framework
EC	European Commission
EEAS	European External Action Service
EEAS report	<i>1st EEAS Report on Foreign Information Manipulation and Interference Threats</i>
EFI	espionage and foreign interference
EIAT	Electoral Integrity Assurance Taskforce
Electoral committee	Joint Standing Committee on Electoral Matters
ENISA	European Union Agency for Cyber Security
Espionage Act	<i>National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018</i>
EU	European Union
FADT committee	Senate Foreign Affairs, Defence and Trade references committee
FIMI	foreign information manipulation and interference
FIS	foreign intelligence services
FITS	Foreign Influence Transparency Scheme
FMIC	Foreign Malign Influence Centre (US)
FORT	Facebook Open Research and Transparency Initiative (Meta)
GDPR	General Data Protection Regulation (EU)
GPS	Global Positioning System
Home Affairs	Department of Home Affairs
HUMINT	human intelligence
IEEE	Institute of Electrical and Electronics Engineers
IEEPA	International Emergency Economic Powers Act (US)
IMSI	International mobile subscriber identity
INGE	Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation
INSLM	Independent National Security Legislation Monitor
IP	Internet protocol
IRI	Islamic Republic of Iran
Law Council	Law Council of Australia

News and Media Research Centre	News and Media Research Centre, University of Canberra
NGO/s	non-government organisation/s
NSW	New South Wales
OpenCTI	Open Cyber Threat Intelligence [platform]
OSINT	open-source intelligence
PCIO	Partnership for Countering Influence Operations
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PR	public relations
PRC	People's Republic of China
PSPF	<i>Protective Security Policy Framework</i>
the Quad	Quadrilateral Security Dialogue between Australia, India, Japan and the US
RESTRICT Act	Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act (US)
SBS	Special Broadcasting Service
SOCI Act	<i>Security of Critical Infrastructure Act 2018</i>
SOCMINT	OSINT gathered from social media platforms
STIX™	Structured Threat Information Expression [data format]
TAG	Threat Analysis Group
Tibetan Association	Australian Tibetan Community Association
ToR	terms of reference
TOR	The Onion Router
TTPs	tactics, techniques and procedures [of threat actors]
TV	television
UFIT	University Foreign Interference Taskforce
UFWD	United Front Work Department (China)
UK	United Kingdom
US	United States of America
VLOP/s	very large online platform/s

Foreword

Foreign interference is now Australia's principal national security threat which risks significantly undermining our values, freedoms and way of life. Australia has been a world leader in combatting foreign interference, however, authoritarian regimes continue to pose an unacceptable risk to democratic societies through targeted online disinformation campaigns that leverage social media platforms to skew public debate, undermine trust in our democratic institutions, and establish narratives that favour the interests of authoritarian states. The proliferation of emerging technologies like artificial intelligence has made their job easier, and demonstrates the need for urgent action to ensure Australia stays ahead of the threat.

Foreign interference is clandestine activity carried out by, or on behalf of, a foreign regime to corrupt our decision-making, political discourse and societal norms. The scale, speed and ease at which these activities can be conducted online means social media is increasingly being weaponised to spread disinformation to deliberately mislead or obscure the truth for malicious or deceptive purposes. Authoritarian regimes like China and Russia are deploying new methods for cyber-enabled disinformation activities as part of a broader, integrated strategic campaign to advance their own national interests at Australia's expense.

Whether we like it or not, social media platforms are today not just the dominant communications channels in modern economies, they constitute the public square for democracies. They are the place where news is first reported, contentious issues are debated, consensus is formed and public policy decisions are shaped. The health of these forums directly affects the health of our democracies.

Foreign authoritarian states know this. They do not permit open and free debates on their own social media platforms. They use ours as a vector for their information operations to shape our decision-making in their national interest—contrary to ours.

Effectively countering foreign interference through social media is therefore one of Australia's most pressing security challenges. That is why on 24 November 2022 the Senate resolved to establish the Select Committee on Foreign Interference through Social Media to investigate the risk posed to Australia's democracy from foreign interference through social media, to expand on the work of the 46th Parliament which investigated cyber-enabled foreign interference.

As the Australian Security Intelligence Organisation (ASIO) rightly assessed, social media itself is not the threat but is a vector for foreign interference. Not all

social media platforms are the same, and therefore the ability for an authoritarian regime to leverage a platform varies greatly for platforms based in authoritarian countries and those that are based in liberal democracies.

The committee was particularly concerned with the unique national security risks posed by social media companies like TikTok and WeChat, whose parent companies ByteDance and Tencent respectively, are irrefutably headquartered in and run from authoritarian countries like China. China's 2017 National Intelligence Law means the Chinese Government can require these social media companies to secretly cooperate with Chinese intelligence agencies. In the case of TikTok, the committee heard that its China-based employees can and have accessed Australian user data, and can manipulate content algorithms—but TikTok cannot tell us how often this data is accessed despite initially suggesting that this information was logged. Nor was TikTok able to provide the legal basis upon which its employees can refuse to comply with Chinese law—the short answer is, it can't.

Throughout the inquiry, the committee found social media companies based in authoritarian countries demonstrated their reluctance to cooperate with Australian parliamentary processes. TikTok was reluctant to provide witnesses sought by the committee, and evasive in their answers when they finally did agree to appear. WeChat showed its contempt for the Parliament by failing to appear before the committee at all, and through its disingenuous answers to questions in writing. This stood in contrast to the more constructive engagement of platforms based in Western countries who at least recognised the fundamental importance of the checks and balances inherent in democratic systems.

The committee was also concerned with the equally serious risk of Western social media companies being weaponised by authoritarian regimes to pump disinformation into our democracy to influence and undermine our political systems. For example, between 2017 and 2022, Facebook's parent company, Meta, disabled more than 200 covert influence operations originating from more than 60 countries that targeted the public domestic debate of another country. In the first quarter of 2023, YouTube terminated more than 900 channels linked to Russia and more than 18 000 linked to China.

In the case of both authoritarian and Western-based social media companies, the committee explored concerns that social media platforms are being used to 'pull' and 'push' information in four ways: to gather intelligence on individuals that will enable them to be targeted; to gather behavioural data by population or cohort to refine interference campaigns; to harass and intimidate Australia's diaspora communities; and to undermine societal trust, spread social disunity and influence decision-making through disinformation campaigns.

Countering this insidious activity becomes more complex as authoritarian regimes continue to adapt and evolve their methods. Emerging new technology and tactics such as the rise of artificial intelligence and the commercialisation of disinformation services, where state actors engage companies to orchestrate disinformation campaigns, threatens to exponentially increase the risk of foreign interference on social media, necessitating an urgent response.

Looking to the future, developing a real-time understanding of and response to foreign interference through social media is critical to protecting our values, freedoms and way of life from interference by foreign regimes. The committee believes that strengthening transparency requirements on social media companies is critical to ensuring they operate with integrity while also preserving the right of Australians to freely communicate and participate in public debate online.

The committee is gravely concerned that the information Australians receive on these platforms is being influenced by directions from foreign authoritarian governments. That's why we have recommended a range of enforceable transparency standards, so that users can both evaluate the content they see on these platforms, and the conduct of the platforms themselves. For example, we believe state-affiliated media entities should be proactively labelled on all platforms. We recommend that any content censored at the direction of a government be disclosed to users. Platforms should be open to independent external researchers who can identify, investigate and attribute coordinated inauthentic behaviour. The access to user data facilitated by these platforms, especially to employees based in authoritarian countries, must be disclosed.

WeChat was found to have comprehensively failed the transparency test by refusing to participate in public hearings on the basis that, despite its significant digital presence, it does not have a physical presence in Australia. The committee therefore recommends that, as part of a suite of transparency requirements, social media companies that operate in Australia be required to establish a physical presence within Australia's legal jurisdiction so that they can be held accountable to our laws.

The committee found that TikTok engaged in a determined effort to obfuscate and avoid answering the most basic questions about the platform, its parent company ByteDance and its relationship to the Chinese Communist Party. That's one reason why the committee has also recommended that social media companies that repeatedly fail to meet the minimum transparency requirements should be subject to fines and, as a last resort, may be banned by the Minister for Home Affairs with appropriate oversight mechanisms in place.

Should the United States Government take action to force ByteDance to divest ownership of TikTok to another company that is not beholden to the Chinese

Communist Party, the committee finds that Australia should consider similar requirements in Australia.

The serious espionage and data security risks posed by TikTok, which necessitated the April 2023 ban on government users downloading the app to their devices, must also be confronted by government contractors and critical infrastructure providers. Government must also put in place measures to anticipate, assess and mitigate the next TikTok before it is widely deployed on government devices.

Deterring this malign online behaviour must be a priority for government. Amended Magnitsky sanctions, bolstered enforcement of espionage and foreign interference offences and support for diaspora communities targeted by transnational repression all need to be part of a package of reforms to raise the costs of this activity.

Of course, social media companies do not need to wait for the government to introduce legislation to strengthen transparency on their platforms. They can proactively undertake this important task on their accord, as some of them are already doing.

Foreign interference through social media is a real, pervasive and growing threat. Despite Australia's world-leading efforts to counter foreign interference including through our Espionage and Foreign Interference statutory framework and the establishment of a Foreign Influence Transparency Scheme, it is evident that there is more work to be done to make Australia an even harder target for the sophisticated disinformation campaigns of authoritarian regimes.

It's not too late to arrest the threat. With a concerted joint effort by government, the private sector and civil society, we can ensure Australia's way of life prevails.

List of recommendations

Recommendation 1

8.43 The committee recommends the Australian Government require all large social media platforms operating in Australia to meet a minimum set of transparency requirements, enforceable with fines. Any platform which repeatedly fails to meet the transparency requirements could, as a last resort, be banned by the Minister for Home Affairs via a disallowable instrument, which must be reviewed by the Parliamentary Joint Committee on Intelligence and Security.

8.44 Requirements should include, at minimum, that all large social media platforms:

- must have an Australian presence;
- must proactively label state affiliated media;
- must be transparent about any content they censor or account takedowns on their platform;
- must disclose any government directions they receive about content on their platform, subject to national security considerations;
- must disclose cyber-enabled foreign interference activity, including transnational repression and surveillance originating from foreign authoritarian governments;
- must disclose any takedowns of coordinated inauthentic behaviour (CIB) networks, and report how and when the platform identified those CIB networks;
- must disclose any instances where a platform removes or takes adverse action against an elected official's account;
- must disclose any changes to their platform's data collection practices or security protection policies as soon as reasonably practicable;
- must make their platform open to independent cyber analysts and researchers to examine cyber-enabled foreign interference activities;
- must disclose which countries they have employees operating in who could access Australian data and keeps auditable logs of any instance of Australian data being transmitted, stored or accessed offshore; and
- must maintain a public library of advertisements on their platform.

Recommendation 2

8.61 The committee recommends that, should the United States Government force ByteDance to divest its stake in TikTok, the Australian Government review this arrangement and consider the appropriateness of ensuring TikTok Australia is also separated from its ByteDance parent company.

Recommendation 3

- 8.69** The committee recommends the Australian Government extend, via policy or appropriate legislation, directives issued under the Protective Security Policy Framework regarding the banning of specific applications (e.g. TikTok) on all government contractors' devices who have access to Australian government data; and
- 8.70** The Minister for Home Affairs should review the application of the Security of Critical Infrastructure Act 2018, to allow applications banned under the Protective Security Policy Framework to be banned on work-issued devices of entities designated of Systems of National Significance.

Recommendation 4

- 8.71** The committee recommends the Australian Government consider extending the Protective Security Policy Framework directive banning TikTok on federal government devices to WeChat, given it poses similar data security and foreign interference risks.

Recommendation 5

- 8.72** The committee recommends the Australian Government continues to audit the security risks posed by the use of all other social media platforms on government-issued devices within the Australian Public Service, and issue general guidance regarding device security, and if necessary, further directions under the Protective Security Policy Framework.

Recommendation 6

- 8.73** The committee recommends the Australian Government establish a national security technology office within the Department of Home Affairs to map existing exposure to high-risk vendors such as TikTok, WeChat and any similar apps that might emerge in the future. It should recommend mitigations to address the risks of installing these applications, and where necessary, ban them from being installed on government devices.

Recommendation 7

- 8.80** The committee recommends the Australian Government designate an entity with lead responsibility for whole-of-government efforts to counter cyber-enabled foreign interference, with appropriate interdepartmental support and collaboration, resources, authorities and a strong public outreach mandate.

Recommendation 8

- 8.82** The committee recommends the Australian Government address countering cyber-enabled foreign interference as part of the *2023–2030 Australian Cyber Security Strategy*.

Recommendation 9

- 8.85** The committee recommends the Australian Government clarify that Magnitsky-style cyber sanctions in the *Autonomous Sanctions Act 2011* can be used to target cyber-enabled foreign interference actors, via legislative amendment if necessary, and ensure it has appropriate, trusted frameworks for public attribution.

Recommendation 10

- 8.90** The committee recommends the Australian Government refer the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* to the Parliamentary Joint Committee on Intelligence and Security for review, with particular reference to the Act's effectiveness in addressing cyber-enabled foreign interference.

Recommendation 11

- 8.94** The committee recommends the Australian Government investigate options to identify, prevent and disrupt artificial intelligence (AI)-generated disinformation and foreign interference campaigns, in addition to the Government's Safe and Responsible AI in Australia consultation process.

Recommendation 12

- 8.97** The committee recommends the Australian Government establish a program of vetting appropriate personnel in trusted social media platforms with relevant clearances to ensure there is a point of contact who can receive threat intelligence briefings.

Recommendation 13

- 8.107** The committee recommends the Australian Government build capacity to counter social media interference campaigns by supporting independent research.

Recommendation 14

- 8.120** The committee recommends the Australian Government ensure that law enforcement agencies, and other relevant bodies such as the eSafety Commissioner, work with social media platforms to increase public awareness of transnational repression.

Recommendation 15

8.124 The committee recommends the Australian Government empower citizens and organisations to make informed, risk-based decisions about their own social media use by publishing plain-language education and guidance material and regular reports and risk advisories on commonly used social media platforms, ensuring this material is accessible for non-English speaking citizens. Specific focus should be on protecting communities and local groups which are common targets of foreign interference and provide pre-emptive information and resources.

Recommendation 16

8.130 The committee recommends the Australian Government support independent and professional foreign-language journalism by supporting journalism training and similar programs, thereby expanding the sources of uncensored news for diaspora communities to learn about issues such as human rights abuses inside their country of origin.

Recommendation 17

8.134 The committee recommends the Australian Government promote the digital literacy and the infrastructure of developing countries in the Indo-Pacific region that are the targets of malicious information operations by foreign authoritarian states.

Chapter 1

Introduction and background

- 1.1 On 24 November 2022, the Senate established the Select Committee on Foreign Interference through Social Media (the committee) to inquire and report on the following matters:
- (a) the use of social media for purposes that undermine Australia's democracy and values, including the spread of misinformation and disinformation;
 - (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 existing Australian laws and regulations; and
 - (e) any other related matters.¹
- 1.2 Details of the inquiry were made available on the committee's webpage and the committee invited organisations, key stakeholders and individuals to provide submissions.²
- 1.3 The committee received 40 submissions, which are listed at Appendix 1 of this report. The committee received a private briefing from government agencies on 20 March 2023 and held the following public hearings for the inquiry:
- 20 April 2023 Canberra—local and overseas subject matter experts;
 - 21 April 2023 Canberra—local and overseas subject matter experts and community-based organisations;
 - 11 July 2023 Canberra—social media companies; and
 - 12 July 2023 Canberra—Australian Government departments and agencies.
- 1.4 A list of the organisations and individuals who attended these public hearings can be found in Appendix 2. The public submissions, additional information received and Hansard transcripts are available on the committee's website.
- 1.5 This inquiry continues the work commenced by the Select Committee on Foreign Interference through Social Media (2019 select committee) established during the 46th Parliament on 5 December 2019. The terms of reference (ToR) for the 2019 select committee were the same as for the current inquiry, with the exception that interference was defined as including the spread of

¹ *Journals of the Senate*, No 22, 24 November 2022, pp. 674–675.

² The committee's webpage is available at: www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_Social_Media/ForeignInterference47

misinformation but not disinformation. This has since been updated in the ToR for this inquiry in the 47th Parliament.

- 1.6 The 2019 select committee tabled an interim report with seven recommendations on 17 December 2021 and a progress report on 21 April 2022. Appendix Three outlines those recommendations and any progress made to implement them, as of early 2023.

Acknowledgement

- 1.7 The committee thanks all those who have contributed to the inquiry by making submissions, providing additional information, and appearing at public hearings.

Report Structure

- 1.8 The report is comprised of eight chapters:
- This chapter, Chapter 1, outlines the conduct and scope of the inquiry, and provides background information on what constitutes foreign interference.
 - Chapter 2 explains how foreign interference manifests in Australia, outlining the experiences of people within Australia who have been subjected to these campaigns.
 - Chapter 3 discusses international responses to counter foreign interference.
 - Chapter 4 outlines current Australian government responses.
 - Chapter 5 discusses ideas for action proposed by evidence to the inquiry.
 - Chapter 6 discusses platform-based responses and gaps.
 - Chapter 7 outlines how government can better support civil society in its responses.
 - Chapter 8 contains the committee comment and recommendations.

Notes on references

- 1.9 References to the Committee Hansard may be references to a proof transcript. Page numbers may differ between proof and official transcripts.

Definitions

- 1.10 Readers should be mindful of the following definitions when considering this report.
- 1.11 **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 a nation's sovereignty, values and national interests.
- 1.12 **Foreign Influence:** overt activities to advocate for particular outcomes or shape consideration of issues important to foreign actors. When conducted in an open and transparent manner, these activities can contribute positively to public debate.

-
- 1.13 **Foreign Information Manipulation and Interference (FIMI):** describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.
- 1.14 **Disinformation:** False information designed to deliberately mislead and influence public opinion or obscure the truth for malicious or deceptive purposes.
- 1.15 **Misinformation:** False information that is spread due to ignorance, by error or mistake with good intentions/without the intent to deceive.
- 1.16 **Coordinated inauthentic behaviour (CIB):** where groups of accounts are used to work together with the intention to deceive others. CIB can be either financially or politically motivated.
- 1.17 **Hybrid warfare:** Hybrid warfare is a military strategy which blends conventional warfare, irregular warfare, and cyberwarfare with other influencing methods, such as fake news, diplomacy, and foreign electoral intervention and lawfare—the use of legal systems and institutions to damage or delegitimise an opponent.
- 1.18 **Cognitive warfare:** The weaponisation of public opinion, by an external entity, for the purpose of (1) influencing public and governmental policy and (2) destabilizing public institutions. 'Cognitive' refers to the manipulation of emotional responses to an issue, which then affects the cognitive function of decision-making regarding that issue.
- 1.19 **OSINT** (open-source intelligence): Publicly available information gathered from the Web to inform an investigative or intelligence cycle.
- 1.20 **SOCMINT:** OSINT gathered from social media platforms.
- 1.21 **Internet/world wide web** is comprised of three layers:
- Surface web: this layer is only four per cent of the internet and is what most people access on a day-to-day basis. It contains all publicly facing websites such as Google services, news sites, blogs, social media and commerce sites.
 - Deep web: this layer is around 95 per cent of the internet and involves data that cannot be indexed by search engines because it contains sites that require logins. For example, sites that contain subscription services, banking, medical or government records.

- Dark web: this is the area of the web containing illegal marketplaces. It must be accessed via special browsers such as TOR (The Onion Router) which provides anonymity.³

What is foreign interference

- 1.22 Foreign interference has been an issue of growing global concern in the past decade. For example, the European Union (EU) Parliament recently declared it was currently 'a target of diverse and aggressive foreign interference campaigns'.⁴
- 1.23 In Australia, the most recent annual threat assessment from the Director-General of the Australian Security Intelligence Organisation (ASIO) stated:
- Australia is facing an unprecedented challenge from espionage and foreign interference and I'm not convinced we, as a nation, fully appreciate the damage it inflicts on Australia's security, democracy, sovereignty, economy and social fabric.⁵
- 1.24 The Department of Home Affairs (Home Affairs) stated that foreign interference 'involves foreign powers trying to secretly and improperly interfere in Australian society to advance their strategic, political, military, social or economic goals, at our expense'.⁶
- 1.25 ASIO submitted that foreign interference 'is particularly insidious in that it uses our strengths against us' and noted that perpetrators 'exploit our values, freedoms and trust, thereby undermining our way of life'.⁷

³ Definitions developed with reference to a range of sources, including: Department of Home Affairs, *Submission 16*; Select Committee on Foreign Interference through Social Media inquiry (46th Parliament), *Interim report*, p. 4; European Union External Action Service, [1st EEAS Report on Foreign Information Manipulation and Interference Threats](#), February 2023, p. 25; Meta, *Submission 32*, p. 6; Weissman, Nilsson, Palmertz and Thunholm, [Hybrid Warfare: Security and Asymmetric Conflict in International Relations](#), Bloomsbury Academic, 2021; Bernal, Carter, Singh, Cao and Madreperla, [Cognitive warfare: an attack on truth and thought](#), NATO OTAN, John Hopkins University, Fall 2020, p. 3; and, Claire Moravec, 'The weaponization of social media', *Security Magazine*, 14 October 2022.

⁴ Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2), [REPORT on foreign interference in all democratic processes in the European Union, including disinformation](#), 2022/2075(INI).

⁵ Mike Burgess Director-General of Security, Australian Security Intelligence Organisation, [Director-General's Annual Threat Assessment](#), 21 February 2023.

⁶ Department of Home Affairs, Defining foreign interference, www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/defining-foreign-interference (accessed 14 July 2023)

⁷ Australian Security Intelligence Organisation, *Submission 2*, p. 2.

1.26 The *Australian Security Intelligence Organisation Act 1979* defines foreign interference as:

- activities relating to Australia that are carried on, by, or on behalf of, are directed or subsidised by, or are undertaken in active collaboration with, a foreign power, being activities that:
 - are clandestine or deceptive, and:
 - are carried on for intelligence purposes;
 - are carried on for the purpose of affecting political or governmental processes; or
 - are otherwise detrimental to the interests of Australia; or
 - involve a threat to any person.
- A foreign power means: a foreign government; an entity that is directed or controlled by a foreign government or governments; or a foreign political organisation.⁸

1.27 Dr Seth Kaplan, a United States (US) politics expert and professorial lecturer at John Hopkins University's School of Advanced International Studies, noted the practical impact of foreign interference:

It basically means that, instead of your democracy being a debate among people who live in the country, there's an additional voice that plays a large part in the conversation, and that voice is controlled by a foreign government that does not have your best interests at heart. I would say that that's the most clear danger. Again, it is basically direct interference in the public square—in the information that people are viewing, in the civil society organisations, in their ability to organise, in what types of civil society organisations might thrive or not thrive.⁹

Foreign interference via social media

1.28 Social media has quickly become a dominant form of communication and information sharing, with 4.62 billion people using social media globally. It is also fast growing, with nearly half a billion users joining social media in 2021 alone.¹⁰

1.29 The Australian Human Rights Commission (AHRC) noted that:

Social media is an integral aspect of everyday life, as it forms the foundation of many Australians' communications online. For example, it was estimated in February 2022 that some 21.45 million Australians (or 82.7% of the

⁸ Australian Security Intelligence Organisation, *Submission 2*, p. 3.

⁹ Dr Seth Kaplan, Private capacity, *Committee Hansard*, 20 April 2023, p. 13.

¹⁰ Claire Moravec, 'The weaponization of social media', *Security Magazine*, 14 October 2022.

population) had active social media accounts, and that 52% of Australians use social media as a source of news.¹¹

- 1.30 The AHRC further noted that 'social media can be used for purposes that both strengthen or undermine Australia's democracy and values', in that social media 'can be used in ways that increase access to information and opportunities for the free exchange of ideas, increase the diversity of voice contributing to public discussions and allow for broader public participation in our democracy', but on the other hand, 'social media can also be used in ways that pose a threat to democratic processes through social media campaigns that spread misinformation and disinformation, undermine trust in public institutions and exacerbate divisions within society'.¹²
- 1.31 Because of its depth and reach into nearly every person's life, social media is being increasingly used as a vector for foreign interference. The DISARM Foundation has warned that 'the internet is enabling the spread and hyper-targeting of disinformation at an unprecedented scale'.¹³
- 1.32 The Federal Bureau of Investigation (US) has noted that:

Foreign influence operations—which include covert actions by foreign governments to influence U.S. political sentiment or public discourse—are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat.¹⁴
- 1.33 The Australian Strategic Policy Institute (ASPI) submitted that social media platforms now form one pillar of the information ecosystem that is 'critical infrastructure for the public to make informed decisions in a functioning democracy, akin to the criticality of the Australian electrical grid supplying power to people's homes'.¹⁵
- 1.34 ASPI further noted that the risks of foreign interference through social media are exacerbated by the changing news consumption habits, where more and more people are using social media platforms as a source of news instead of mainstream news outlets, and advised that 'this has implications for the Australian Government's ability to regulate and cooperate with social media

¹¹ Australian Human Rights Commission, *Submission 9*, p. 4.

¹² Australian Human Rights Commission, *Submission 9*, p. 3.

¹³ DISARM Foundation, *What's this all about*, www.disarm.foundation/disinformation (accessed 17 May 2023).

¹⁴ Federal Bureau of Investigation, *Combating Foreign Influence*, www.fbi.gov/investigate/counterintelligence/foreign-influence (accessed 14 July 2023).

¹⁵ Australian Strategic Policy Institute, *Submission 13*, p. 7.

platforms that share fewer values in common - such as transparency - and may have less power to influence'.¹⁶

Misinformation and disinformation

1.35 A recent EU report analysing foreign interference and FIMI found that:

- **Diplomatic channels are an integral part of FIMI incidents.** Russia's diplomatic channels regularly serve as enablers of FIMI operations. They are deployed across a wide range of topics. China also uses diplomatic channels, mostly targeting the US.
- **Impersonation techniques become more sophisticated.** Impersonations of international and trusted organisations and individuals are used by Russian actors particularly to target Ukraine. Print and TV [television] media are most often impersonated, with magazines seeing their entire style copied.
- **FIMI actor collusion exists but is limited.** Official Russian actors were involved in 88 analysed FIMI incidents. Chinese actors were involved in 17. In at least five cases, both actors engaged jointly.
- **FIMI is multilingual.** Incidents do not occur in just one language; content is translated and amplified in multiple languages. Incidents featured at least 30 languages, 16 of which are EU languages. Russia used a larger variety of languages than Chinese actors but 44% of Russian content targeted Russian-speaking populations, while 36% targeted English-speaking populations.
- **FIMI is mostly intended to distract and distort.** Russia (42%) and China (56%) mostly intend to direct attention to a different actor or narrative or to shift blame ("distract"). Russia attempts to change the framing and narrative ("distort") relatively more often (35%) than China (18%).
- **FIMI remains mostly image and video based.** The cheap and easy production and distribution of image and video material online makes these formats still the most commonly used.¹⁷

Social media as part of wider foreign interference

1.36 Foreign interference through social media does not occur in isolation. ASIO has summarised the issue of foreign interference via social media as follows:

Social media is a vector for foreign interference, not a threat in and of itself. However, foreign powers seek to do Australia harm through a variety of vectors and capabilities, including social media platforms, often as part of a broader campaign and an invariably integrated one.¹⁸

¹⁶ Australian Strategic Policy Institute, *Submission 13*, p. 6.

¹⁷ European Union External Action Service, [*1st EEAS Report on Foreign Information Manipulation and Interference Threats*](#), February 2023, p. 5.

¹⁸ Australian Security Intelligence Organisation, *Submission 2*, p. 2.

1.37 Dr William Stoltz, a national security professional and academic, told the committee that:

... any instances of foreign interference that are occurring via social media are typically going to be linked to a larger strategic objective and are therefore also going to be part of a larger suite of statecraft, both overt and covert, that a state would be undertaking.¹⁹

1.38 Professor Rory Cormac, from the University of Nottingham, noted that because of this, it was important that governments not be 'blinded by the novelty of the technology and forget the wider history and the wider concepts that states have learned over the years of foreign subversion and interference'.²⁰

Foreign interference for economic outcomes

1.39 Foreign interference can be conducted by state actors as part of a wider push to influence other nation states, but it can also be conducted to seek economic outcomes. Ms Lindsay Gorman of the Alliance for Securing Democracy explained that:

We know that China and Russia—especially China—have very active espionage campaigns against liberal democracies to steal information, both in the traditional national security sense and also in the corporate espionage sense.²¹

1.40 CyberCX submitted that its intelligence has assessed that 'several foreign governments have the intent and capability to use social media to harm Australia's economic interests, and tactics can include 'social media disinformation or data breach operations designed to harm the value or reputation of a company, or to pressure a company or its executives to change their policies or views'.²²

1.41 By way of example, Home Affairs noted reports that Australian mining company Lynas Rare Earths was targeted by an information operation seeking to undermine efforts to diversify global rare-earth supply chains.²³

1.42 The following chapter outlines how foreign interference is manifesting in Australia.

¹⁹ Dr William Stoltz, Private capacity, *Committee Hansard*, 20 April 2023, p. 37.

²⁰ Professor Rory Cormac, Director, Centre for the Study of Subversion, Unconventional Interventions and Terrorism, University of Nottingham, *Committee Hansard*, 20 April 2023, p. 37.

²¹ Ms Lindsay Gorman, Senior Fellow for Emerging Technologies, Alliance for Securing Democracy, German Marshall Fund, *Committee Hansard*, 21 April 2023, p. 13.

²² CyberCX, *Submission 16*, p. 6.

²³ Department of Home Affairs, *Submission 1*, p. 4. See also CyberCX, *Submission 16*, p. 4.

Chapter 2

Foreign interference in Australia

Foreign interference in Australia

2.1 Just as foreign interference is a key security concern of nations elsewhere, it is a key concern in Australia. The Department of Home Affairs (Home Affairs) submitted that:

Foreign interference and espionage is the principal security concern facing Australia. Foreign interference and espionage threaten the things that we value most about our country: our social cohesion, our trusted democracy, and our freedoms. Australia remains a target of sophisticated and persistent foreign interference activities directed towards government, academia, industry, the media and our communities. The nature and scale of the threat we face is complex, and undermines our sovereignty, values and national interests.¹

2.2 The following sections will outline the four key areas of foreign interference that are of concern in Australia, two related to the pull of information and two related to the push of information. The fears are that social media platforms and applications (apps) can be used to:

- gather intelligence on individuals that can be used to target them;
- gather behavioural data by population or cohort that can be used to improve interference and influence campaigns;
- harass Australia's diaspora communities; and
- spread misinformation or disinformation with the intent to:
 - achieve a specific outcome within Australia's political system;
 - manipulate community discourse and understanding about an issue; or
 - spread chaos and seed distrust in Australia's democratic systems.

2.3 Chapter 1 outlined that foreign interference via social media can be part of a wider campaign of interference. This has also been experienced in Australia. For example, Mrs Kateryna Argyrou, Co-Chair of the Australian Federation of Ukrainian Organisations, spoke of Russian interference tactics being used against the Ukrainian diaspora community in Australia as always evolving and coming from all angles, using social media to support real-world interference. Mrs Argyrou described the formation of support groups ostensibly to support Ukrainians, but which were in fact established by Russian background people who used the groups to gather data on Ukrainians residing in Australia.²

¹ Department of Home Affairs, *Submission 1*, p. 3.

² Mrs Kateryna Argyrou, Co-Chair, Australian Federation of Ukrainian Organisations, *Committee Hansard*, 21 April 2023, p. 29.

- 2.4 Badiuca, a Chinese-born Australian artist who is a well-known dissident against the Chinese Communist Party (CCP), agreed that social media-based interference is often just one of the tactics in a wider interference campaign. He told the committee:

Recently, I also find they are being bolder and aggressive. In February this year, I actually got approached by a person who claimed to be a journalist of Reuters. Eventually, I found out that this is not the person he claimed to be. When I verified with real Reuters journalists, we found out this is not the person. It turned out there are three different persons' accounts from Telegram channelled into Twitter, pretending to be the entire China bureau of Reuters. They are using this fake identity to trick dissidents and the Chinese diaspora outside of China, including inside China, to send sensitive information about human rights campaigns and other political opinion.³

Gathering intelligence on individuals

- 2.5 Prior to the prevalence of social media, human intelligence (HUMINT) was painstakingly gathered by 'travel, articles, public events, and old fashioned boots on the ground surveillance'. However, social media has now become the primary source of HUMINT, given the numbers of people posting intimate details of their public and professional lives:

- 59 per cent of people post names or photos of children.
- 27 per cent of people post names or photos of their partner.
- 93 per cent of people post employment updates.
- 36 per cent of people post information about their company job, boss, colleagues.
- 32 per cent of people post updates and photos during business trips.
- Around 55 per cent of people do not have privacy settings activated on their social media.⁴

- 2.6 This issue of concern is outlined in greater detail later in this chapter, when discussing interference against specific members of diaspora communities in Australia, and concerns related to the professional networking site, LinkedIn, is discussed in Chapter 6.

Gathering behavioural data

- 2.7 A key concern for the mass gathering of behavioural data via apps such as TikTok, is that it enables microtargeting of advertising and influence campaigns, which can then be used to engage in foreign interference.
- 2.8 Internet 2.0 submitted that big data is one of China's stated primary fields for strategic competition, and that China sees big data as 'a new opportunity to reshape its competitive advantage'. Internet 2.0 further noted that '[e]ffective

³ Badiuca, Private capacity, *Committee Hansard*, 21 April 2023, p. 33.

⁴ Claire Moravec, 'The weaponization of social media', *Security Magazine*, 14 October 2022.

disinformation campaigns also rely on high quality data to have insight into voting patterns.⁵

2.9 This issue of concern is discussed in greater detail in Chapter 6, *Platforms*.

Harassment of diaspora communities in Australia

2.10 Social media platforms are being used to facilitate the transnational repression of individuals and marginalised communities in Australia. The Australian Strategic Policy Institute (ASPI) observed that:

This poses a significant threat to the freedom of Australians, and others residing in Australia, to express their opinion and access online spaces ... On social media, this includes online trolling, stalking or harassment, and is typically conducted by authoritarian states to coerce their citizens and others abroad.⁶

2.11 Four diaspora communities in Australia are currently known to be subject to significant surveillance and interference by foreign state actors: Iranians, Chinese, Tibetans and Ukrainians.

2.12 The impact of this foreign interference on the lives of individuals cannot be overstated. Ms Vicky Xu, a journalist and policy analyst told the committee that:

... I'm still dealing with death threats. I'm still dealing with repeated hacking attempts. Just this week I received a dozen hacking attempts across all of my accounts ... I've had to adapt the way I live, my lifestyle, to one that's akin to a criminal, I would say. People in democracies, politicians, academics and people with good social standing tell me things like I'm going to end up in history books, and that all sounds grand, but what about life? I'll just leave it at that.⁷

Iran

2.13 There have been many recent media reports of harassment or surveillance of Iranians in Australia, specifically targeting dissidents who speak out against the current Iranian regime.

2.14 In one case, the mother of a leading Iranian-Australian protester was jailed in Tehran and interrogated about her Australian relatives in what her family and experts fear is part of a wider attempt to silence Australia's Iranian pro-democracy protesters. Iranian-Australians say they do not feel safe from the Iranian regime even inside Australia's borders. Several activists said local

⁵ Internet 2.0, *Submission 17*, p. 3 and 6.

⁶ Australian Strategic Policy Institute, *Submission 13*, p. 3.

⁷ Ms Vicky Xu, Senior Fellow, Australian Strategic Policy Institute, *Committee Hansard*, 21 April 2023, p. 35.

protests had sometimes turned violent after people suspected of being linked to the Iranian regime arrived and filmed them.⁸

2.15 The Minister for Home Affairs and Minister for Cyber Security advised the Australian public in February 2023 that ASIO 'disrupted the activities of individuals who had conducted surveillance in the home of an Iranian-Australian'.⁹

2.16 Mr Peter Murphy, Co-secretary of Australian Supporters of Democracy in Iran, told the committee that 'it's very, very clear that in Iran the state controls the mainstream media and has also invested heavily in cyberwarfare, cybersurveillance and creating its own messaging apps to enable it to monitor dissident opinions and communicate its own "information"'.¹⁰

2.17 Mr Murphy further told the committee:

The basics of our [Australia's] democratic society include freedom of association, freedom of speech and freedom of expression, and this family in Melbourne has been told to stop talking, stop attending certain meetings and stop expressing certain views. It is really a blatant attack on our basic rights by a foreign government.¹¹

2.18 The Australian Supporters of Democracy in Iran submitted that most cybersecurity efforts in Australia do not specifically relate to political interference through social media. They argued that 'this is an area of policy and governance which is under-developed, including in Australia'.¹²

2.19 A recent expert study commissioned by the European Parliament noted that 'Iran is among the actors who focus on "laundering disinformation" through seemingly legitimate front and proxy media' and further argued that these 'operations will remain untouched by measures targeting fake accounts or inauthentic behaviour'. The study recommended a dedicated taskforce, fact-checkers and sanctions against malicious actors, but noted that 'sanctions would have to be preceded by appropriate investigations in order to identify those who should be sanctioned'.¹³

⁸ Paul Sakkal, '[Silencing dissent by threatening family: Iran cracks down on family of Australian protester](#)', *The Sydney Morning Herald*, 16 January 2023.

⁹ Minister for Home Affairs and Minister for Cyber Security, Hon Clare O'Neil MP, '[Foreign Interference in Australia – ANU address](#)', 14 February 2023.

¹⁰ Mr Peter Murphy, Co-Secretary, Australian Supporters of Democracy in Iran, *Committee Hansard*, 21 April 2023, p. 20.

¹¹ Mr Peter Murphy, Australian Supporters of Democracy in Iran, *Committee Hansard*, 21 April 2023, p. 22.

¹² Australian Supporters of Democracy in Iran, *Submission 23*, p. 4.

¹³ Directorate General for External Policies of the Union, '[The misuse of social media platforms and other communication channels by authoritarian regimes: Lessons learned](#)', December 2021, p. 45.

Senate inquiry: Human Rights implications of recent violence in Iran

2.20 The Senate Foreign Affairs, Defence and Trade references committee (FADT committee) recently tabled a report into politically motivated violence in Iran. This inquiry received a significant volume of evidence from effected individuals, with a total of nearly 400 submissions. The committee expressed concerns at 'reports of threats and intimidation against Australian residents and citizens' and noted the 'high level of concern within the Iranian Australian diaspora about potential monitoring of individuals on social media, as well as at rallies and protests held in Australia'.¹⁴

2.21 The FADT committee further noted that Home Affairs and the Australian Federal Police advised that reports of such intimidation and threats would be investigated where it reached a criminal threshold. The FADT committee made three recommendations on this issue:

- that the responsible Ministers provide an update to the Parliament and the Australian public on the government's current assessment of whether persons connected to the Islamic Republic of Iran (IRI) regime are undertaking such behaviour in Australia;
- that the Australian Government ensure there is an appropriate level of expertise and resourcing in the relevant government departments and agencies, including foreign language speakers and community liaison officers, available to quickly investigate and assess threats against Australians; and
- that all reports of threats, intimidation, monitoring or surveillance by the Iranian community in Australia are followed up, recorded, assessed and reported to the lead coordination agency (regardless of whether individual reports result in a criminal investigation) to ensure that the government has a complete picture of foreign interference efforts by the IRI in Australia. The committee further recommended that the relevant agencies report to Parliament through the Joint Committee for Intelligence and Security on such activities.¹⁵

Russia

2.22 The committee was told about Russian-backed influence and interference campaigns are occurring in Australia. Mrs Kateryna Argyrou of the Australian Federation of Ukrainian Organisations, told the committee 'we have many members of our community that have been targeted by either the Russian community or the Russian consulate here'. Mrs Argyrou said the targeting was:

¹⁴ Senate Foreign Affairs, Defence and Trade References Committee, [*Human Rights implications of recent violence in Iran*](#), p. 49.

¹⁵ Senate Foreign Affairs, Defence and Trade References Committee, *Human Rights implications of recent violence in Iran*, pp. 38–51.

... quite varied, anything from direct death threats through social media, mostly coming through Telegram and Facebook where certain people, especially community leaders, are targeted in the most vile way. They basically describe how they would be executed, beheaded, where their head is going to end up and so on and so forth. It's very confronting.¹⁶

- 2.23 Mrs Argyrou further stated that community concerns around COVID-19 have been used as a tactic for influence campaigns:

They've found a very innovative and interesting way to do that, where they target different subgroups in Australia to try to influence opinion and perception. For example, through ... the Russian consulate and Russian agents in Australia they have been very successful in infiltrating the antivax movement. First, they learn about the ideals and aims of a certain movement. They share those ideals and views, and they quickly become leaders of that and through that they place typical Russian narratives and propaganda. They have been very successful in infiltrating that antivax movement here in Australia, and that's just one example.¹⁷

China

- 2.24 The committee received a great deal of evidence of the CCP engaging in interference in Australia, both via social media and in real-world events.

- 2.25 Badiucac, a Chinese-born Australian dissident artist told the committee:

I have been receiving death threats almost on a daily basis. That has just been a burden on me every day. The Chinese government know that the only way that they can stop dissidents overseas from talking about the important human rights issues is by launching character assassination campaigns.¹⁸

- 2.26 Badiucac further told the committee with regard to WeChat:

... WeChat has become this very toxic headquarters for misinformation and propaganda for the Chinese government, but at the same time for users, no matter whether you're inside China or outside China in Australia, the rate for free speech to survive is zero.¹⁹

- 2.27 Ms Vicky Xu, a journalist and policy analyst told the committee that:

... the Chinese government has been attempting to silence, intimidate and harass me ... Because of my reporting on [Hong Kong protests]—whether that's orchestrated by someone or whether that's just voluntary sort of anger from the people, I don't know—a large online social harassment campaign

¹⁶ Mrs Kateryna Argyrou, Australian Federation of Ukrainian Organisations, *Committee Hansard*, 21 April 2023, pp. 27–28.

¹⁷ Mrs Kateryna Argyrou, Australian Federation of Ukrainian Organisations, *Committee Hansard*, 21 April 2023, p. 27.

¹⁸ Badiucac, Private capacity, *Committee Hansard*, 21 April 2023, p. 33.

¹⁹ Badiucac, Private capacity, *Committee Hansard*, 21 April 2023, p. 35.

occurred on the platform called Weibo. It had such an impact on my family life that I became estranged from my father.²⁰

- 2.28 Ms Xu told the committee that social media played a large role in this character assassination 'because there are hundreds of accounts pumping out content that goes across the entirety of the Chinese internet, so from WeChat and Weibo to the Chinese version of Quora, which is Zhihu, and to the video platforms'.²¹
- 2.29 Dr Seth Kaplan noted the dangers that Chinese social media platforms and apps pose to the Australian-Chinese community:

... the Chinese diaspora in Australia, the Chinese Australians, are a vulnerable community because of how their information is being managed, and that information prevents many voices from being heard. It prevents many civic activities or civil society organisations forming and/or developing. It creates tensions within the community because only certain voices, which could be more extreme on the left or right or could simply be saying very negative [things].²²

Tibet

- 2.30 Mr Kalsang Tsering, President of the Australian Tibetan Community Association (Tibetan Association), told the committee of the plight of Tibetan-Australians being monitored by the CCP in Australia:

There are about 3,000 Tibetans all over Australia. Tibetan communities have been persecuted, and we are not able to freely contact our families back in Tibet. Most of the Tibetans in Australia are former political prisoners; or their parents or siblings are former political prisoners. Almost everyone, 90 per cent of us, have families back in Tibet, and we cannot freely communicate with them.²³

- 2.31 The Tibetan Association submitted a range of alleged human rights abuses by the CCP against Tibetan-heritage people in Australia, including instances of surveillance, interference, and repression of freedom of expression, association, and the right to protest. The association also claimed that bots are used to spread CCP information, misinformation and disinformation, disseminate disunity, as well as to attack posts in support of Tibet.
- 2.32 The Tibet Association claimed that some of these actions have been taken through social media applications, including WhatsApp, Twitter, Facebook, and WeChat (used by Tibetans and Chinese overseas and in Australia) and through phone calls and messages.

²⁰ Ms Vicky Xu, Australian Strategic Policy Institute, *Committee Hansard*, 21 April 2023, p. 34.

²¹ Ms Vicky Xu, Australian Strategic Policy Institute, *Committee Hansard*, 21 April 2023, p. 34.

²² Dr Seth Kaplan, Private capacity, *Committee Hansard*, 20 April 2023, p. 15.

²³ Mr Kalsang Tsering, President, Australian Tibetan Community Association, *Committee Hansard*, 21 April 2023, p. 24.

- 2.33 The Tibetan Association discussed the action taken against Tibetans and their families including harassment, fear, intimidation, death threats and actions against family in Tibet. It also claimed that Tibetan community members in Australia have become increasingly suspicious and paranoid of each other as a result of this work. Mr Tsering stressed this impact directly to the committee, stating:

It is a very big thing for us to communicate freely, because we were born in Tibet and came to Australia as a second home. We want to speak about the atrocities and the human rights violations in Tibet, but we cannot speak freely. Still, we feel that it's our duty, in a free country like Australia, to speak about what is happening inside Tibet. As we do that, the Chinese government even tries to go through our phones or laptops and tries to get information about us, and then they try to persecute, question or detain our families back home.²⁴

China—global concerns

- 2.34 Information considered by the committee strongly suggests that the Australian examples above are not happening in isolation, and are not only happening to diaspora communities. They are occurring as part of a global interference and influence campaign by the CCP, that has been decades in the making and has the potential to inflict seismic shifts in geopolitical stability.
- 2.35 A recent joint address was made by the heads of Security Service MI5 (United Kingdom) and the Federal Bureau of Investigation (United States). It was the first time the heads of those agencies had shared a public platform, and they came together 'to send the clearest signal we can on a massive, shared challenge: China'. The address made the following key points:
- The CCP is covertly applying pressure across the globe. Rather than lone actors it is a coordinated campaign on a grand scale, and involves planned, professional activity to conduct a strategic contest across decades.
 - The CCP adopts a whole-of-state approach in which businesses and individuals are forced by law to cooperate with the Party.
 - President Xi said that in areas of core technology where it would otherwise be impossible for China to catch up with the West by 2050, they 'must research asymmetrical steps to catch up and overtake'.
 - The CCP doesn't just use intelligence officers posing as diplomats in the classic fashion. Privileged information is gathered on multiple channels, in what is sometimes referred to as the 'thousand grains of sand' strategy.
 - The Chinese intelligence services, or bodies within the CCP itself—such as its United Front Work Department—are mounting patient, well-funded, deceptive campaigns to buy and exert influence.

²⁴ Mr Kalsang Tsering, Australian Tibetan Community Association, *Committee Hansard*, 21 April 2023, p. 24.

- Countering state threats needs a profound whole-of-system response, bringing together not just the national security community but counterparts in economic and social policy, in industry, in academia.²⁵

2.36 In its February 2023 report on foreign interference, the European Union External Action Service identified the CCP as a:

... multifaceted FIMI [foreign information manipulation and interference] actor with an arsenal that is diverse and includes various tactics. Its activities range from benign – public diplomacy – to clearly illegitimate – intimidation and harassment of critical voices with the aim of suppressing information also outside of its borders.²⁶

2.37 The report outlined that China has been seen using its own state-controlled media and economic leverage over other media outlets to influence media coverage in its own interests, while simultaneously suppressing critical stories using 'a wide range of often covert tactics, including intimidating and harassing individuals, also targeting overseas Chinese communities'.²⁷

2.38 An ASPI report into cyber-enabled foreign interference found that:

The Chinese Communist Party (CCP) has invested US\$6.6 billion into its global media presence since 2009. It has run covert information operations on Silicon Valley social media platforms since at least 2017. The party invests in global data collection on a massive scale, and its external propaganda is increasingly precisely targeted to granular international audience segments.²⁸

2.39 The ASPI report pointed to statements by Chinese President Xi Jinping that clearly outlined this intent and noted that 'the CCP is strategically and deliberately building an international-facing propaganda system that's designed to reshape the international order'.²⁹

2.40 Ms Lindsay Gorman of the Alliance for Securing Democracy noted the increasing use of social media by the CCP to achieve these strategic objectives. Ms Gorman told the committee:

... over the last five years, PRC [People's Republic of China] diplomats and state media outlets have flocked to social media to spread China's message

²⁵ Security Service MI5, *Joint Address by MI5 and FBI Heads*, 6 July 2022, www.mi5.gov.uk/news/speech-by-mi5-and-fbi (accessed 14 July 2023)

²⁶ European Union External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, February 2023, p. 10.

²⁷ European Union External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 10.

²⁸ Ms Danielle Cave and Dr Jacob Wallis, '[Cyber-enabled foreign interference](#)', *Strategic Insights*, November 2022, p. 20.

²⁹ Ms Danielle Cave and Dr Jacob Wallis, '[Cyber-enabled foreign interference](#)', *Strategic Insights*, November 2022, pp. 20–21.

to the world, increase its discourse power, denigrate the United States and the international world order, and position itself as an alternative democracy.³⁰

2.41 Mr Fergus Ryan of ASPI similarly told the committee:

The Chinese Communist Party and propaganda officials see a unique opportunity in the world at the moment, where the internet has disrupted traditional media. They see social media as an outlet that they can use to close the gap when it comes to China's soft power versus the West's soft power. These activities have been taking place on Facebook, on Twitter and on YouTube, and, as you said, there have been efforts to identify that activity that's taking place.³¹

2.42 Internet 2.0 described how authoritarian regimes, including China, 'know the value of the data, and have moved to collect it on us and limit our access to it in their social media domain' and 'conduct mass surveillance through social media within their own borders'. Internet 2.0 went further to state that applications such regimes build are purpose-built for surveillance and when they 'export these business models to our social media environments the legacy of this surveillance culture permeates'.³²

2.43 Ms Yaqiu Wang, a Senior China Researcher with Human Rights Watch told the committee that China broadens its intelligence gathering reach by coercing private companies and using them as tools for political purposes:

The CCP has a record of compelling domestic and foreign companies to toe the party line and of punishing those who fail to sufficiently do so. It has forcefully disappeared a score of business executives under murky circumstances, a practice that has only increased in recent years under President Xi Jinping... this sends a clear message to business leaders in China that the price of opposing, or even appearing to oppose, the CCP can be extraordinarily steep.³³

2.44 Ms Shanthi Kalathil, a former advisor on the United States (US) National Security Council, told the committee of relevant Chinese laws:

There are a number of data laws that are relevant to this issue, including the 2015 National Security Law, the 2017 National Intelligence Law, the 2017 national Cybersecurity Law and the Data Security Law. The lack of a

³⁰ Ms Lindsay Gorman, Senior Fellow for Emerging Technologies, Alliance for Securing Democracy, German Marshall Fund, *Committee Hansard*, 21 April 2023, p. 8.

³¹ Mr Fergus Ryan, Analyst, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 20.

³² Internet 2.0, *Submission 17*, p. 5.

³³ Ms Yaqiu Wang, Senior China Researcher, Human Rights Watch, *Committee Hansard*, 21 April 2023, p. 1.

meaningful barrier between private enterprise and the demands of the party state is less a technical or legal issue than a political issue.³⁴

- 2.45 Meta also provided commentary on changes in approach and an overall escalation of coordinated inauthentic behaviour (CIB) originating from China:

... we have seen quite a shift in tactics and approach by China based actors over the past seven months or so. Fifty per cent of the China-originating CIB networks we have actioned in the last four years we've taken down in the last seven months. We are seeing a whole range of new tactics evolving, such as operations that are linked to troll farms; attempts to co-opt journalists, NGOs [non-government organisations] or other respected third parties; and attempts to work through PR [public relations] firms.³⁵

Case study: Mr Kenny Chiu

- 2.46 According to an independent thinktank, the Council on Foreign Relations, China has pursued a pattern of influence operations in the Pacific Rim to shift narratives toward China's points of view, promote pro-China politicians, or sometimes just to sow chaos and falsehood. US law enforcement authorities warned about such interference in the 2022 midterm elections and both Google and Meta's cybersecurity arms have warned of Chinese online interference in the midterms.³⁶
- 2.47 Raising similar concerns about north American election meddling, Canadian Security Intelligence Service documents revealed that China had employed a sophisticated strategy to defeat Conservative Party politicians considered to be unfriendly to Beijing in the 2021 federal election in Canada. The tactics included disinformation campaigns, undeclared cash donations and the use of international Chinese students studying in Canada, as campaign volunteers to support preferred Liberal Party candidates.³⁷
- 2.48 The committee heard directly from Mr Kenny Chiu, a former Canadian member of parliament who said China's alleged election meddling is the reason he lost his seat in the 2021 Canadian federal election.
- 2.49 In 2021, Mr Chui introduced a private members bill which proposed a Foreign Influence Registry to require 'individuals acting on behalf of a foreign principal to file a return when they undertake specific actions with respect to public office holders'. The purpose of the bill became the target of a misinformation campaign. Mr Chiu also had a background in parliament of

³⁴ Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, p. 2.

³⁵ Mr Josh Machin, Head of Public Policy, Australia, Meta, *Committee Hansard*, 11 July 2023, p. 3.

³⁶ Joshua Kurlantzick, '[China's Growing Interference in Domestic Politics: Globally and in the United States](#)', *Council on Foreign Relations*, 1 November 2022.

³⁷ Robert Fife and Steven Chase, '[CSIS documents reveal Chinese strategy to influence Canada's 2021 election](#)', *The Globe and Mail*, 22 February 2023.

advocating for Hong Kong and democracy, and criticising Beijing's violations of human rights, as well as urging the Canadian government to impose sanctions on China.³⁸

2.50 Mr Chiu reported that during the 2021 federal campaign, he discovered WeChat stories circulating which claimed that his private members bill would put Chinese-Canadians in danger. Mr Chui alleged efforts to oust candidates seen as unfriendly to Beijing, and stated he was targeted by pre-election disinformation on Chinese-language social media.³⁹

2.51 Mr Chiu told the committee:

It started before the election, and during the election we started seeing authoritative articles being written and circulated among the WeChat community which both attacked my then leader, Mr Erin O'Toole, and specifically also used my private member's bill to attack me. The articles claimed that we were anti-Chinese, that we were Chinese haters and that therefore we must be opposed. They said that should I get re-elected again, my bill would somehow automatically be passed, and all Chinese in Canada would be subject to unimaginable Chinese exclusion and persecution. This disinformation was activated soon after the election started and came with a ferocity that, frankly speaking, was not what I had anticipated or expected, so we were caught unprepared.⁴⁰

2.52 Media reporting also appears to suggest the interference campaign went unnoticed by the body established by the Canadian government to 'monitor threats to federal elections'. The Security and Intelligence Threats to Elections Taskforce is reported to have issued no public warnings about any campaigns and advised the Prime Minister that it had found no evidence of interference, reporting to parliament that it had 'determined that the integrity of our elections was not compromised in 2019 or 2021'.⁴¹ However, it appears that since 2021 foreign interference threats to democratic elections in Canada have only grown.⁴²

Interference in Australian politics

2.53 Internet 2.0 submitted that authoritarian regimes seek to interfere in elections within liberal democracies not just to promote preferred candidates, but also

³⁸ Sze-Fung Lee and Benjamin Fung, '[Misinformation and Chinese interference in Canada's affairs](#)', *Policy Options*, 4 January 2022.

³⁹ Chuck Chiang, '[Canada has become "open market" for foreign interference in elections, former Conservative MP says](#)', *The Canadian Press*, 18 February 2023.

⁴⁰ Mr Kenny Chiu, Private capacity, *Committee Hansard*, 21 April 2023, p. 15.

⁴¹ Robert Fife and Steven Chase, '[CSIS documents reveal Chinese strategy to influence Canada's 2021 election](#)', *The Globe and Mail*, 22 February 2023.

⁴² See, for example: Steven Chase, '[A timeline of China's alleged interference in recent Canadian elections](#)', *The Globe and Mail*, 9 March 2023 (accessed 26 July 2023).

simply to reduce confidence of the population in the true results of elections. It stated that by 'conducting divisive campaigns, they seek to divide our societies, to weaken us, and to fracture our uniting values'.⁴³

2.54 CyberCX agreed, noting that 'disinformation and misinformation need not change the outcome of an election, but merely raise the spectre of illegitimacy'.⁴⁴

2.55 During the Australian Security Intelligence Organisation (ASIO) annual threat assessment in 2022, the Director-General advised:

... espionage and foreign interference has supplanted terrorism as our principal security concern ... The threat is pervasive, multifaceted and, if left unchecked, could do serious damage to our sovereignty, values and national interest.

I can confirm that ASIO recently detected and disrupted a foreign interference plot in the lead-up to an election in Australia.

2.56 The Director-General provided details of the attempted foreign interference. A wealthy individual with direct and deep connections to a foreign government and its intelligence agencies hired and financed an employee to identify candidates likely to run in the election who either supported the interests of the foreign government or who were assessed as vulnerable to inducements and cultivation. These candidates were then supported through financial donations and promoted in positive media stories in Australian foreign language media. The purported aim was to exploit successful candidates' sense of indebtedness and to manipulate them to the advantage of the foreign government.

2.57 ASIO intervened and harm was avoided. However, ASIO suggested a scenario of possible outcomes from a successful interference of this nature:

Some of the candidates get elected. The puppeteer's employee then recommends they hire certain other associates as political staffers. These people are also agents or proxies of the foreign government, and will try to influence the politician, shape decision-making and help identify other political figures who can be influenced and recruited. Down the track, the new parliamentarians might be asked for information about the party's position on defence policy, human rights, foreign investment or trade. This information will be sent to the foreign power without the knowledge of the parliamentarian. At some point, the politicians might be prevailed upon to vote a particular way on a contentious issue, or lobby colleagues to vote a certain way.⁴⁵

⁴³ Internet 2.0, *Submission 17*, p. 6.

⁴⁴ CyberCX, *Submission 16*, p. 2.

⁴⁵ Australian Security Intelligence Organisation, [*Director-General's Annual Threat Assessment*](#), 9 February 2022.

Tactics

2.58 The following section outlines some of the key tactics used in foreign interference through social media. Actions being taken to address these are described in Chapter 6, which looks in-depth at social media platforms.

Misinformation and disinformation

2.59 Misinformation and disinformation are key concerns in this space, however ASIO noted that they are distinguished from each other on the basis of intent: misinformation is false or misleading content spread due to ignorance or by mistake, while disinformation also involves false or misleading content with an intention to cause harm or deceive.⁴⁶

Box 2.1 Department of Foreign Affairs and Trade, *Our Work: Disinformation & Misinformation*

The increasing ubiquity of cyberspace and social media platforms as a source of information and for personal engagement on a wide range of social and community issues has made them a key venue for the dissemination and amplification of disinformation and misinformation.

Disinformation may be used as a tool for foreign interference. Foreign actors continue to spread disinformation to serve their own strategic interests and to undermine public trust in democratic institutions and confidence in official messaging, disrupt the proper functioning of open media, or undermine social cohesion.

Recent electoral processes around the world have shown that digital disinformation campaigns have low barriers to entry, and that malicious actors have effectively hijacked public discourse to influence communities and broader public opinion on matters of significant importance. Unwittingly, platforms designed to promote openness have been misappropriated to promulgate and amplify disinformation and misinformation, sow division and mistrust, and ultimately pervert public discourse.

Malicious use of critical technologies is increasingly occurring to amplify these campaigns. This includes 'bots' that drown out legitimate online debate, data-driven technologies that enable malicious or harmful micro-targeting of susceptible and/or influential audiences, and machine learning-enabled 'deep fakes' that spread disinformation.

Disinformation should be differentiated from foreign influence. All governments can seek to influence discussions on issues of importance. When conducted in an open and transparent manner, foreign influence can

⁴⁶ Australian Security Intelligence Organisation, *Submission 2*, p. 3.

contribute positively to public debate and form a legitimate part of international engagement.⁴⁷

- 2.60 As outlined above, disinformation can be spread by foreign state actors for the purposes of influencing election outcomes, influencing decision-making, targeting diaspora communities or simply to spread chaos and create dissent.
- 2.61 Australians are most likely to see disinformation on larger digital platforms, like Facebook and Twitter. However, smaller private messaging apps and alternative social media services are also increasingly used to spread disinformation or conspiracies due to their less restrictive content moderation policies.⁴⁸ Because foreign interference by social media takes place on commonly used and trusted platforms, it is hard for laypeople to detect when going about their business online.
- 2.62 The following sections discuss how misinformation and disinformation is spread online.

Algorithms

- 2.63 The use of algorithms on social media is ubiquitous. These programs run in the background of platforms like Facebook, Twitter and YouTube, analysing what material a user is interested in and tailoring their social media feed to gather as much of the user's time and attention as possible. While what appears on a social media feed can feel 'natural', these recommender systems and algorithms can actually be used to not only identify people's interests but also manipulate their emotions.
- 2.64 The eSafety Commissioner recently developed a position statement on recommender systems and algorithms which stated that 'while recommender systems and algorithms have positive uses, they can also present an array of risks to users' one of which is to 'amplify harmful and extreme content, particularly when used by platforms whose content feeds are driven by user engagement'. The eSafety Commissioner further noted that this can normalise 'prejudice and hate and distrust in public institutions' and may also 'contribute to radicalisation towards terrorism, violent extremism, and provide users with avenues to find associated groups'.⁴⁹
- 2.65 In a submission to the inquiry held in the 46th Parliament, Responsible Technology Australia described how these algorithms were

⁴⁷ Department of Foreign Affairs and Trade, *Our Work: Disinformation & Misinformation*, www.internationalcybertech.gov.au/our-work/security/disinformation-misinformation (accessed 17 January 2023).

⁴⁸ Australian Communications and Media Authority, *A report to government on the adequacy of digital platforms' disinformation and news quality measures*, June 2021, p. 1.

⁴⁹ eSafety Commissioner, *Submission 10*, p. 1.

initially developed to sell advertisements, but now have been found to often have the unintended effect of promoting 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.⁵⁰

Micro-targeting

- 2.66 While the use of algorithms described above could be described as a 'normal' part of the experience of being on social media platforms, micro-targeting is the weaponisation of the social media environment to further the goals of various actors—corporate, international or even malicious actors. 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.⁵¹

- 2.67 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.'⁵²

Bots

- 2.68 A common method of foreign interference and/or influence on social media is the use of 'bots'. Bots (short for 'robots') are artificial social media accounts that mimic the behaviour of real users, spreading misinformation or otherwise enacting whatever function they have been designed to carry out. Bots are:

... 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

⁵⁰ Responsible Technology Australia, *Submission 17: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 2.

⁵¹ Responsible Technology Australia, *Submission 17: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 2.

⁵² Joint Standing Committee on Electoral Matters, [*Report on the conduct of the 2016 federal election and matters related thereto*](#), November 2018, p. 176.

follower numbers, supporting political campaigns, or spreading misinformation and disinformation.⁵³

- 2.69 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 misinformation and disinformation online.
- 2.70 A related online phenomenon is a 'rumour cascade', which bots can assist in propagating. A rumour cascade begins when a singular user makes an assertion, leading to other propagating the rumour and retweeting it. Researchers have found that 'false news spreads more pervasively than the truth online', which is still mainly perpetrated by human users, as opposed to bots.⁵⁴

Troll farms

- 2.71 Troll farms (or factories) create multiple fake social media profiles to conduct disinformation propaganda activities on the Internet, usually focused on the political or economic sphere, for example, attacking political opponents or other action indicated by the ordering party. Troll farms achieve their goals using, among other things, fake news and hate speech.⁵⁵
- 2.72 The committee was told of that in April 2023, US prosecutors charged 34 officers of China's Ministry of Public Security with operating a troll farm to attack Chinese dissidents, sow division and disseminate disinformation. The committee heard that prosecutors 'allege that the officers were part of an elite task force called the 912 Special Project Working Group and that the group created thousands of fake profiles on social media sites, including Twitter, and spread propaganda about topics like human rights in Hong Kong and the Xinjiang region'.⁵⁶

Content farms

- 2.73 Content farms use similar tactics as troll farms, by creating multiple fake 'news' sites that appear to be separate entities but are in fact jointly operated and coordinated. They are profit driven to generate traffic and advertising revenue and usually distribute entertainment-based content, 'articles about politics and current affairs are also common, especially if news events are sensational or high

⁵³ House of Commons (United Kingdom), Digital, Culture, Media and Sport Committee, [Disinformation and 'fake news': Interim report](#), 29 July 2018, p. 19.

⁵⁴ Soroush Vosoughi, Deb Roy and Sinan Aral, '[The spread of true and false news online](#)', *Science*, 9 March 2018, Volume 359: 6380, pp. 1146–1151.

⁵⁵ North Atlantic Treaty Organization (NATO), [Media – \(Dis\)Information – Security](#), pp. 1–2.

⁵⁶ Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, p. 2.

profile'. Content farms can then be 'leveraged by state actors to disseminate propaganda or manipulate how the reporting of events is framed'.⁵⁷

Emerging Tactics

2.74 Three new tactics that have the potential to exponentially increase foreign interference through social media are now emerging: the establishment of companies that offer fee-based interference services; the development of artificial intelligence; and, the increasing decentralisation of social media apps.

Foreign Interference as a fee-service

2.75 A report by the Oxford Internet Institute in early 2021 highlighted the existence of disinformation-as-a-service. Then in 2023, another report highlighted the emergence of foreign interference-as-a-service.

2.76 In early 2021 the Oxford Internet Institute reported that disinformation had become 'a common strategy of cyber manipulation' and reported that of the 'organised social media manipulation campaigns' found to operate in 81 countries, 'more than 76 of these campaigns deployed disinformation as part of political communication'. One of the report's authors noted that:

Our 2020 report highlights the way in which government agencies, political parties and private firms continue to use social media to spread political propaganda, polluting the digital information ecosystem and suppressing freedom of speech and freedom of the press. A large part of this activity has become professionalized, with private firms offering disinformation-for-hire services.⁵⁸

2.77 The Oxford Internet Institute's researchers found:

- Private 'strategic communications' firms are playing an increasing role in spreading computational propaganda, with researchers identifying state actors working with such firms in 48 countries.
- Almost \$60 million has been spent on firms who use bots and amplification strategies to create the impression of trending political messaging.
- Social media has become a major battleground, with firms such as Facebook and Twitter taking steps to combat 'cyber troops', while some \$10 million has been spent on social media political advertisements. The platforms removed more than 317 000 accounts and pages from 'cyber troops' actors between January 2019 and November 2020.⁵⁹

⁵⁷ Dr Wallis, Bogle, Zhang, Mansour, Niven, Ho, Liu, Dr Ong, and Dr Tapsell, '[Influence for hire](#)', *Strategic Insights*, Policy Brief Report No. 48/2021, 10 August 2021, p. 17.

⁵⁸ Oxford Internet Institute, '[Social media manipulation by political actors now an industrial scale problem prevalent in over 80 countries – annual Oxford report](#)', *Media release*, 13 January 2021.

⁵⁹ Oxford Internet Institute, 'Social media manipulation by political actors now an industrial scale problem prevalent in over 80 countries – annual Oxford report', *Media release*, 13 January 2021.

- 2.78 In early 2023 a global group of reporters working together uncovered an outfit—referred to in reporting as 'Team Jorge'—that provided hacking and disinformation services and had allegedly actively interfered in the electoral processes of 33 elections around the world. The investigation and subsequent reporting on the scale and scope of the group's activities highlighted that foreign-interference-as-a service had well and truly arrived.
- 2.79 An article reporting on the group's activities observed that 'in the past, online disinformation campaigns appeared to work in isolation', but Team Jorge operated differently:

What's so powerful about this example is that they're not just doing the disinformation, they're also involved in 'on the ground' operations. That's a really dangerous combination ... As an example: reporters were able to identify a fake protest staged outside a company headquarters in London where masked protesters filmed themselves waving placards – a stunt that was then circulated on social media.⁶⁰

Artificial intelligence

- 2.80 Artificial intelligence (AI) is expected to have an exponential impact on foreign interference and disinformation campaigns. Internet 2.0 submitted:

Artificial intelligence will enable disinformation campaigns as it exponentially increases the computation and distribution of high quality information ... The implications of artificial intelligence, if it is not regulated in its use within journalism, elections, and the media, are that our authoritarian adversaries will have the advantage in the information domain.⁶¹

- 2.81 Ms Shanti Kalathil noted that foreign interference 'is about to take a significant turn into the unknown anyway, with the advent of generative AI and other advances'. Ms Kalathil advised that:

... we are behind the curve in equipping society's populations and educational institutions and other key components of civil society with the knowledge and resilience to pass information in this age. There's no easy solution to this issue, but at a minimum we must be better prepared to confront even more potent forms of information manipulation than what we have already encountered.⁶²

- 2.82 Ms Lindsay Gorman of the Alliance for Securing Democracy outlined the dangers that AI presents for foreign interference:

Deepfake images, video and text can enable automated propaganda. The rise of content that looks plausible but is not necessarily true also runs the risk of undermining broader trust in the information environment, which is

⁶⁰ Archie Bland, '[Thursday briefing: The secret disinformation group who claim to influence elections worldwide](#)', *The Guardian*, 16 February 2023 (accessed 26 July 2023).

⁶¹ Internet 2.0, *Submission 17*, p. 6.

⁶² Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, p. 2.

critical for quality information to flourish in democracies. As democracies contemplate regulation on AI, restoring trust in the information environment and guarding against authoritarian information manipulation should be at the forefront of these conversations.⁶³

2.83 Mr David Robinson of Internet 2.0 argued that AI 'is increasing the effectiveness of influence and disinformation campaigns against elections' and that when combined with high quality data 'we cannot guarantee we can defend ourselves and we will not be able to reverse the loss of trust our system will suffer'.⁶⁴

2.84 Mr Robinson further noted the impact that AI will have on democracy:

Social media is so important in elections because people make decisions based on what the group is saying or doing, and government makes decisions in its normal running based on what it thinks the population wants. [However] a social media platform with AI and botnets can create hundreds of thousands of accounts and talk about the same issue. That influences what you as lawmakers and politicians and what the population do and say to each other. I think AI is very dangerous, and if we don't have laws to regulate how it acts on social media—about talking about elections, for example—I think we're running out of time, to be honest. I think it's the most dangerous thing.⁶⁵

2.85 The Australian Signals Directorate similarly advised the committee that AI poses risks through its ability to 'speed up the capacity' of cyber-based attacks.⁶⁶ Home Affairs noted that the Department of Industry is the coordinating body for the current project which is 'forming a whole-of-government position on the opportunities and risks associated with AI', with Home Affairs providing the 'national security policy advice informing that decision-making' including by 'partnering with research institutions to understand the policy parameters and techniques that currently exist in perpetrating or proliferating the threat'.⁶⁷

Meta Threads and decentralisation

2.86 Launched on 5 July 2023 by Meta, Threads is touted as a decentralised version of Twitter and signed up 30 million users in its first day. A key aspect of decentralisation is the ability for users to host their own instances or servers, giving greater control over their data (including apps Lens Protocol, Mastodon and Steemit). While Threads does not currently offer this option, technology

⁶³ Ms Lindsay Gorman, Alliance for Securing Democracy, *Committee Hansard*, 21 April 2023, p. 9.

⁶⁴ Mr David Robinson, Director, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 31.

⁶⁵ Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 35.

⁶⁶ Ms Abigail Bradshaw, Deputy Director-General, Australian Signals Directorate, *Committee Hansard*, 12 July 2023, p. 14

⁶⁷ Mr Peter Anstee, Acting First Assistant Secretary, Department of Home Affairs, *Committee Hansard*, 12 July 2023, p. 15.

writers note that Meta may incorporate these features in their future.⁶⁸ However, even in its current state, Threads is not currently available in the European Union because it does not comply with safety regulations.⁶⁹

2.87 Threads has been noted to collect more user data than Twitter:

Threads is collecting almost everything it can, including data on your health, purchases, financial info, location, contact info, search history, and browsing history.⁷⁰

eSafety concerns with a decentralised internet

2.88 The eSafety Commissioner published a position statement on a decentralised internet with the following summary:

Under a decentralised internet, often referred to as 'DWeb' or 'Web 3.0', users are said to have more power because they can access online services and platforms without relying on a concentration of large technology companies that own or operate mainstream, centralised servers (the computer hardware and software that stores data).

While decentralisation can allow users to protect their information and control their online experiences, it can also make it more difficult to hold users (or the entities behind them) responsible for illegal and harmful content and conduct

2.89 The eSafety Commissioner noted some positives of decentralisation:

- Decentralisation could improve the security, privacy and autonomy of online users by giving them greater control over their personal information and online experiences.
- Decentralisation could also enhance freedom of expression and protect diversity of thoughts and opinions and reduce the risk of monitoring, tracking and targeting of at-risk or marginalised individuals or groups, including whistle-blowers and advocates for social change.

2.90 Risks identified by the eSafety Commissioner included:

- The absence of centralised servers and lack of central authority, along with the storage and distribution of data across many computers, makes it difficult to moderate or regulate decentralised services and platforms or enforce the removal of illegal and harmful content. A decentralised internet

⁶⁸ Jojo Percs, 'How decentralized is Threads? Not at all for now', *Medium*, 8 July 2023, https://medium.com/@jojo_percs/how-decentralized-is-threads-not-at-all-for-now-87279710539e (accessed 10 July 2023).

⁶⁹ Dan Milmo, 'Threads app: Instagram owner's Twitter rival logs 5 million users in first hours', *The Guardian*, 6 July 2023.

⁷⁰ Stan Schroeder, 'Threads, Meta's Twitter rival, is tracking you in all sorts of ways', *Mashable*, 6 July 2023, <https://mashable.com/article/threads-tracking-data> (accessed 10 July 2023).

may become a haven for criminal activities and for users who have been removed from mainstream services and platforms.

- It would be up to communities on each platform to decide and apply standards, with a risk that unchecked online environments can allow a range of harms from abuses to grow, without providing any way for users to get help or for consequences to be imposed on those responsible.
- The inability to enforce standards for conduct and content within a decentralised internet may actually harm freedom of expression instead of improving it.
- Using decentralised services may give users more control over their information and online experiences, but it also increases their own responsibility for understanding and operating in unregulated environments and keeping their personal information secure.

2.91 The eSafety Commissioner recommended that adopting a *Safety by Design* approach when developing decentralised platforms can mitigate these risks, by including protections such as:

- community moderation;
- opt-in governance;
- identity verification; and
- content moderation.⁷¹

⁷¹ eSafety, *Decentralisation—position statement*, www.esafety.gov.au/industry/tech-trends-and-challenges/decentralisation (accessed 10 July 2023).

Chapter 3

International issues

- 3.1 As outlined in Chapter 1, foreign interference, through social media and other methods, is an issue affecting liberal democracies around the world. This chapter outlines some of the main countermeasures being undertaken in nations and regions which are key security partners of Australia: the European Union (EU) and the nations which—with Australia—make up the 'Five Eyes' intelligence alliance: the United States, Canada, United Kingdom and New Zealand.
- 3.2 Finally, the chapter outlines security risks in the Pacific region and looks at a few examples of international digital literacy campaigns.

Europe

- 3.3 In recent years, the EU has been contending more and more with the issue of social media and cyber-enabled foreign interference, alongside the related threats of cyber-security, data security and privacy. As early as 2015, the European Council was publicly stressing 'the need to challenge Russia's ongoing disinformation campaigns' and called for 'an action plan on strategic communication'.¹

European Union Agency for Cyber Security

- 3.4 The European Union Agency for Cyber Security (ENISA), published a report in December 2022, *Foreign Information and Interference (FIMI) and Cybersecurity—Threat Landscape*. The report outlines how the concept of FIMI has been proposed as a response to the call of the *European Democracy Action Plan* for 'refined common definitions and methodologies in order to address different categories of disinformation and influence activities.' The report states:

Although disinformation is a prominent part of FIMI, FIMI puts emphasis on manipulative behaviour, as opposed to the truthfulness of the content being delivered ... one of the main motivations behind this report is to identify ways to bring the cybersecurity and counter-FIMI communities closer together. The ambition is to provide an input to the on-going and ever pressing discussion on the nature and dynamics of information manipulation and interference, including disinformation, and on how to collectively respond to this phenomenon. The report proposes and tests an analytical approach describing FIMI and manipulation of information, as

¹ European Council conclusions, 20 March 2015, [EUCO 11/15](#), p. 5.

well as the underlying cybersecurity elements, by combining practices from both domains.²

- 3.5 This approach is now replicated across many EU agencies, which tend to define interference activities based on outcomes sought rather than tactics being used: focus is directed to the overall goals of the interference—manipulation of the information environment—as opposed to whether the information itself is misinformation or disinformation.

European Parliament

Special committee on Foreign Interference

- 3.6 The first Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE 1), was established in 2020. INGE 1 was tasked to report on factual findings and recommendations concerning the measures and initiatives to be taken in countering foreign interference and disinformation.
- 3.7 After eighteen months of work—including 50 hearings with over 130 invitees—the report of the committee identified and mapped the threat of foreign interference in all its forms and provided a diagnosis of the EU's vulnerabilities and recommendations for strengthening the EU's resilience.³
- 3.8 INGE 2 was established in 2022 with a revised mandate to follow up on the implementation of the INGE 1 report, and to engage in a dialogue with policy makers at the national, the European and the international levels to contribute to the overall institutional resilience against foreign interference, hybrid threats and disinformation in the run-up to European elections in 2024.
- 3.9 Since May 2022, INGE 2 has spoken with as many as two dozen experts and policy makers. In order to best focus on institutional and legislative resilience building in the run-up to European elections in 2024, INGE 2 established a close cooperation with North Atlantic Treaty Organization StratCom in Riga (Latvia), the Hybrid Centre of Excellence in Helsinki (Finland), with the Australian Government, and authorities and respective bodies at the United Nations in New York.
- 3.10 The INGE 2 report included recommendations and updates on the EU's coordinated strategy against foreign interference; on EU resilience building; on interference using online platforms; on the critical infrastructure and strategic sectors; on interference during electoral processes; on covert funding of political activities by foreign actors and donors; on cybersecurity and resilience of

² European Union Agency for Cyber Security, *Foreign Information and Interference (FIMI) and Cybersecurity—Threat Landscape*, December 2022, p. 4.

³ Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 1), *REPORT on foreign interference in all democratic processes in the European Union, including disinformation*, ([2020/2268\(INI\)](#)).

democratic processes; on the impact of interference on the rights of minorities and other vulnerable groups; on deterrence, attribution and collective countermeasures, including sanctions; and on neighbourhood policy, global cooperation, and multilateralism.⁴

EU Digital Services Act

3.11 Passed in 2022 and in force from 1 January 2024, the *Digital Services Act* updates and harmonises the legal framework for regulating illegal content – including disinformation – on digital intermediaries across the EU and co-regulates platforms along with the 2022 *Code of Practice on Disinformation* (EU code). The Digital Services Act requires all online platforms with more than 45 million European users (known as Very Large Online Platforms, or VLOPs) to have measures in place to mitigate risks from the spread of illegal content', with 'different purposes and enforcement remedies [through the EU code], depending on whether an organisation is a VLOP or another category of organisation'.⁵

European Commission – tackling online disinformation

3.12 As part of its *European Democracy Action Plan* and complementary to the *General Data Protection Regulation*, the European Commission (EC) issued a *Communication on Tackling online disinformation: a European approach in 2018*.⁶ As part of this approach, the EC committed to a range of initiatives to address disinformation across the EU, including through making online platforms more accountable, such as:

- recognition of the voluntary EU code, strengthened further in 2022, including misinformation into the code scope, and measures demonetising pedlars of disinformation, transparency of political advertising, reducing manipulative behaviour, better informing users, expanding fact-checking coverage, and improving transparency and reporting;
- developing the *Action Plan against Disinformation*⁷; and
- establishing the European Digital Media Observatory – independent fact checkers and independent researchers.

⁴ Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2), *REPORT on foreign interference in all democratic processes in the European Union, including disinformation*, 2022/2075(INI).

⁵ Australian Communications and Media Authority, *Submission 6*, p. 3; Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Submission 7*, p. 3; European Commission, *The Digital Services Act package*, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (accessed 2 March 2023).

⁶ European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling online disinformation: a European approach*, 24 April 2018, pp. 1–16.

⁷ European Commission, *Action Plan against Disinformation*, 5 December 2018.

3.13 In February 2023 a Transparency Centre was announced including baseline reports on actions taken by major online platforms in response to disinformation.⁸ In relation to the baseline reports, the EC noted that:

Most major online platforms (Google, Meta, TikTok and Microsoft) demonstrated strong commitment to the reporting, providing an unprecedented level of detail about the implementation of their commitments under the Code, and—for the first time—data at Member State level. Twitter, however, provides little specific information and no targeted data in relation to its commitments.⁹

3.14 Reports from online platforms referenced foreign interference matters, including in relation to elections, the 'war of aggression by Russia on Ukraine', and Commitment 16 relating to cross-platform influence operations and foreign interference.¹⁰

European External Action Service

3.15 The European External Action Service (EEAS) is the EU diplomatic service. In 2015, the EEAS established its own disinformation unit—East StratCom Task Force—following the calls outlined above for greater action against disinformation. Since then, a number of reports and initiatives have been undertaken, as outlined below.

EUvsDISINFO

3.16 In 2015, East StratCom Task Force launched a project, *EUvsDiSInfo*, 'to increase public awareness and understanding of the Kremlin's disinformation operations, and to help citizens in Europe and beyond develop resistance to digital information and media manipulation'. *EUvsDiSInfo* states that it uses 'data analysis and media monitoring services in 15 languages, *EUvsDisinfo* identifies, compiles, and exposes disinformation cases originating in pro-Kremlin media that are spread across the EU and Eastern Partnership countries'.¹¹

⁸ Australian Communications and Media Authority, *Submission 6*, p. 3; European Commission, *Tackling online disinformation*, <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation> (accessed 1 March 2023).

⁹ European Commission, *Signatories of the Code of Practice on Disinformation deliver their first baseline reports in the Transparency Centre*, <https://digital-strategy.ec.europa.eu/en/news/signatories-code-practice-disinformation-deliver-their-first-baseline-reports-transparency-centre> (accessed 1 March 2023).

¹⁰ See, for example: TikTok, *Code of Practice on Disinformation—Report of TikTok for the period 16 June–16 December 2022*, pp. 51, 77 and 143.

¹¹ EUvsDisInfo, *About*, <https://euvsdisinfo.eu/about/> (accessed 7 July 2023).

EEAS Report on Foreign Information Manipulation and Interference Threats

3.17 In June 2022, a workshop of high-level experts from civil society, industry, and government was convened to take stock of best practices in the FIMI analyst community by the Carnegie Endowment for International Peace. That workshop identified a key barrier to addressing FIMI was the lack of agreed upon definitions and analytical standards for analysing and reporting on FIMI.¹²

3.18 Following on from that workshop, the EEAS released the *1st EEAS Report on Foreign Information Manipulation and Interference Threats* (EEAS report) in February 2023 to:

... provide the FIMI defender community with a proof-of-concept for a common framework that enables mutual sharing of complex insights in a timely fashion and at scale. This is done to create a common understanding and formulate a collective, systematic response to FIMI.¹³

3.19 The EEAS report had three main components:

- a pilot FIMI threat analysis on priority actors and issues in 2022;
- a behaviour-first approach to FIMI detection and analysis, as well as the linked DISARM 'Kill Chain' perspective on FIMI; and
- an analytical framework for FIMI threat analysis.¹⁴

3.20 The EEAS report proposed using the Disinformation Analysis and Risk Management (DISARM) open-source framework, which is:

... designed for describing and understanding the behavioural parts of FIMI/disinformation. It sets out best practices for fighting disinformation through sharing data & analysis, and can inform effective action. The Framework has been developed, drawing on global cybersecurity best practices.¹⁵

3.21 The DISARM framework builds on the ABCDE framework of differentiating FIMI incidents 'in terms of actors, behaviours, content, degree, and effect' which is seen as a 'helpful mnemonic for both investigators and readers to check whether an analysis covers every important aspect of a FIMI incident'. The DISARM framework goes further, to articulate an analysis cycle that is self-reinforcing, in that 'the more often the analytical workflow is applied, the better informed each research iteration will become':

¹² Carnegie Endowment for International Peace, *Partnership for Countering Influence Operations*, <https://carnegieendowment.org/specialprojects/counteringinfluenceoperations/> (accessed 15 May 2023).

¹³ European Union External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 5.

¹⁴ EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 7.

¹⁵ EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 4.

Figure 3.1 Self-reinforcing workflow for strategically analysing incidents of Foreign Information Manipulation and Interference



Source: European Union External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 27.

- 3.22 The EEAS report noted the importance of taking a systematic approach to developing countermeasures, as well as then measuring the success of different strategies.¹⁶
- 3.23 The EEAS report also emphasised the importance of ensuring countermeasures are appropriate to the seriousness of the particular threat, noting that the point of countering FIMI is to protect the integrity of the democratic process and universal values. For example, where anonymity is a key tactic of a FIMI actor, government responses must 'weigh whether challenging that central feature of the internet is proportionate to tackling the risk'.¹⁷
- 3.24 The EEAS report identified a range of countermeasures that can be taken to address FIMI:
- **Statement of Refutation:** An involved entity issued a statement refuting the claims of the incident.
 - **Debunking:** The claims of the incident were debunked/fact-checked.

¹⁶ EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 26.

¹⁷ EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 26.

- **Content Deleted:** Content of any type was taken down in response to the incident.
- **Content Confined:** Content of any type was limited in response to the incident.
- **Channel Limited or Suspended:** The channel of any of the observables was limited or suspended in response to the incident.
- **Other:** Any other counter measure that is not captured by the above taxonomy.¹⁸

3.25 The EEAS report highlighted an additional tactic to the above, which is to use a 'Kill Chain' approach as modified by the DISARM Foundation for use against FIMI. This approach recognises that a single FIMI incident has many necessary steps—planning, creating and disseminating content—and to deny a threat actor any one of those steps effectively kills off the attack:

This approach builds upon positive experience in cybersecurity, where the forensic analysis of threat actor behaviour throughout the entire timeline of their attempted attack has helped to better understand systemic vulnerabilities, and how to spot and close their exploitation to prevent the infiltration of and damage to computer systems.¹⁹

3.26 Most importantly, the Kill Chain approach acknowledges that each step of the FIMI chain requires not only different approaches to detection and analysis, but also requires different countering strategies and techniques.²⁰

3.27 Figure 3.2 below shows the four identified stages of a FIMI incident, each of which then allows for a different strategy and techniques to disable that stage and 'kill' the entire incident:

¹⁸ EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 24.

¹⁹ EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 26.

²⁰ EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 26.

Figure 3.2 DISARM Foundation – Kill Chain



Source: EEAS, 1st EEAS Report on Foreign Information Manipulation and Interference Threats, p. 29.

Visualisation of the DISARM framework's threat actor Kill Chain (Red Team). Red dots represent the overarching tactics (TA) at a given stage, blue dots show examples of techniques (T) used under a given tactic.

- 3.28 The EEAS report noted that in order for a Kill Chain approach to be helpful, it must be supported by objective analysis of the behaviour and tactics, techniques and procedures (TTPs) threat actors use, as well as systematic development and measurement of disruptive responses.²¹
- 3.29 The EU Agency for Cyber Security noted that having a community of multiple FIMI countermeasure actors from different sectors enables any response to be tailored by choosing the best political actor to respond to a specific FIMI event.²²
- 3.30 The EEAS report also found that large-scale collaboration required a 'common data format for sharing threat information' that was 'able to represent all fundamental building blocks (or objects) of a threat and express how they are related to one another'. The report further noted of FIMI data standards:

It would also have to be flexible enough to remain useful while the threat keeps evolving, but stable enough to allow for the adaptation of processes and the building of tools on top of it. Lastly, it should follow the same principles of openness, community involvement and universality as commonly shared taxonomies to find wide adoption.²³

- 3.31 The report recommended the adoption of the existing *Structured Threat Information Expression* (STIX™) format used for cyber threat information, and

²¹ EEAS, 1st EEAS Report on Foreign Information Manipulation and Interference Threats, p. 26.

²² EEAS, 1st EEAS Report on Foreign Information Manipulation and Interference Threats, p. 26.

²³ EEAS, 1st EEAS Report on Foreign Information Manipulation and Interference Threats, p. 30.

suggested it be updated to STIX2.1 with custom extensions needed for idiosyncratic FIMI threat indicators.²⁴

- 3.32 Notably, on 31 May 2023, the EU-United States (US) Trade and Technology Council announced it has adopted the DISARM and STIX2 frameworks as 'a common standard for exchanging structured threat information on FIMI':

This standard that the European Union and the United States are now using to analyse FIMI and share information is comprised of the DISARM framework, the STIX2 standard and the OpenCTI [open cyber threat intelligence] platform. This approach will significantly strengthen our collective efforts to identify, analyse and counter FIMI by enhancing our common situational awareness of FIMI threats. At the same time, this standard and its elements are made up of open-source solutions, which is key to ensure an approach that can be used by stakeholders around the globe.²⁵

Information Sharing and Analysis Center

- 3.33 Announced on 7 February 2023, the EU has launched a new platform to counter disinformation campaigns by Russia and China. The *Information Sharing and Analysis Center* within the EEAS will track information manipulation by foreign actors and coordinate with the 27 EU countries and the wider community of non-government organisations (NGOs). It will be a decentralised platform to exchange information in real-time with NGOs, countries and cybersecurity agencies, enabling better understanding of emerging disinformation threats and narratives and quicker action to tackle such problems.²⁶

TikTok in the EU

TikTok bans

- 3.34 The European Parliament, EC, and the EU Council, the three top EU bodies, have all banned TikTok on staff devices, citing cybersecurity concerns. Individual EU nations that have imposed similar bans as of 4 April 2023, include France, the Netherlands, Norway and Denmark.²⁷

Project Clover

- 3.35 As part of its efforts to allay fears about misuse of user data and privacy concerns, TikTok has begun what it refers to as Project Clover, which the

²⁴ EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, p. 30.

²⁵ EEAS, Trade and Technology Council, [Trade and Technology Council Fourth Ministerial – Annex on Foreign information manipulation and interference in third countries](#), 31 May 2023, p. 1.

²⁶ Clothilde Gioujard, ['EU to launch platform to fight Russian, Chinese disinformation'](#), *Politico*, 7 February 2023.

²⁷ Euronews, ['Which countries have banned TikTok and why?'](#), 4 April 2023.

company said in an 8 March 2023 statement builds on its data approach in the US, writing:

... we are further enhancing these controls by introducing security gateways that will determine employee access to European TikTok user data and data transfers outside of Europe. This will add another level of control over data access. Any data access will not only comply with the relevant data protection laws but also have to first go through these security gateways and additional checks.²⁸

3.36 TikTok also reported that it was working on additional privacy enhancing technologies that included 'pseudonymisation of personal data so that an individual cannot be identified without additional information and aggregation of individual data points into large data sets to protect the privacy of individuals'.

3.37 TikTok also announced a number of European data centre sites in Europe as part of what it said was its 'commitment to store European TikTok user data locally', outlining that it would begin storing European user data locally in 2023, with migration continuing into 2024, at an overall cost of €1.2 billion.²⁹

Agreement between EU and United States on transatlantic cooperation

3.38 In May 2023, the EU and the US announced a number of actions to increase transatlantic cooperation to proactively address FIMI and disinformation:

- *Common methodology for identifying, analysing and countering FIMI*
The EU and the US have adopted a common standard for exchanging structured threat information on FIMI, through a more interoperable and machine-readable approach. When fully operational, information will be shared more efficiently, effectively and with a greater level of detail when it comes to understanding the manipulative tactics, techniques and procedures. This standard that the EU and the US are now using to analyse FIMI and share information is comprised of the DISARM framework, the STIX2 standard and the OpenCTI platform.
- *Enhancing the preparedness against FIMI in third countries together with Civil Society Organisations (CSOs) and platforms*
The EU and the US organised several workshops to bring together civil society organisations, academic institutions, and media outlets from Africa and Latin-America, as well as platforms active in these regions, to explore how a multi-stakeholder community can step up its actions in coordinating the response to FIMI.
The EU and the US intend to further enhance support for capacity building in third countries, including by exploring additional actions to support and

²⁸ TikTok, *Setting a new standard in European data security with Project Clover*, 8 March 2023, <https://newsroom.tiktok.com/en-ie/project-clover-ireland> (accessed 16 July 2023).

²⁹ TikTok, *Setting a new standard in European data security with Project Clover*.

reinforce civil society and fact-checking organisations that facilitate the fight against FIMI on online platforms through our respective development funding mechanisms.

- *Call for action to platforms*

The EU and the US also called upon online platforms to ensure the integrity of their services and to effectively respond to disinformation and FIMI, building on the example of the EU's updated *Code of Practice on Disinformation*.³⁰

United States

Foreign Malign Influence Centre

3.39 The Foreign Malign Influence Centre was established in September 2022. It is housed under the Director of National Intelligence and 'serves as the primary U.S. Government organization for analysing and integrating all intelligence and other reporting possessed or acquired pertaining to foreign malign influence, including election security'.³¹

Department of State – Global Engagement Centre

3.40 The mission of the Global Engagement Centre of the Department of State is to 'direct, lead, synchronize, integrate, and coordinate U.S. Federal Government efforts to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations'.

3.41 It does this through five areas of work:

- (a) **Analytics and Research:** collects data to produce analysis on foreign malign information influence narratives, tactics, and techniques, which is then shared with domestic and international partners.
- (b) **International Partnerships:** with other national governments for the purpose of coordinating counter-disinformation analyses and actions.
- (c) **Programs and Campaigns:** has issue specific teams to build societal and institutional resilience to foreign propaganda and disinformation efforts.
- (d) **Exposure:** has a coordination role in the exposure of foreign information influence operations.

³⁰ US EU Joint Statement of the Trade and Technology Council, [Annex 3](#), 29 May 2023.

³¹ Director of National Intelligence (US), The National Counterterrorism Center, *Foreign Malign Influence Center Fact Sheet*, www.dni.gov/files/FMIC/documents/FMIC_Fact_Sheet.pdf (accessed 16 July 2023).

- (e) **Technology Assessment and Engagement:** assesses counter-disinformation technologies against specific challenges, and identifies technological solutions through technology challenge programs.³²

TikTok & WeChat IEEPA Orders

- 3.42 In August 2020, President Trump attempted to use powers under the *International Emergency Economic Powers Act* to ban TikTok and WeChat in the US, or to force ByteDance's divestment of TikTok to a non-Chinese company. A court case struck down the Executive Orders, which were subsequently withdrawn by President Biden.³³

RESTRICT ACT

- 3.43 In response to the executive orders being struck out by legal challenges, on 7 March 2023 a bipartisan group of 13 US Senators introduced a bill that would create the Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act, which has been referred to a US Senate Committee for inquiry. The RESTRICT Bill creates an entirely new legislative framework that would allow the Secretary of Commerce to review and regulate foreign-linked tech firms for national security risks and then develop mitigating options.³⁴

TikTok ban

- 3.44 In late December 2022, the US government approved a ban on the use of TikTok on government owned devices. Reporting from February 2023 indicates TikTok has been banned from state government owned devices in half of the states, and a number of universities in the US are also reported to have banned the use of TikTok on their networks.³⁵

Project Texas

- 3.45 Project Texas is similar to Project Clover, in that the US \$1.5 billion project with technology company Oracle is designed to ensure that TikTok US user data remains stored in the US. However, whistleblowers have raised concerns that

³² US Department of State, *About Us – Global Engagement Center*, www.state.gov/about-us-global-engagement-center-2/ (accessed 16 July 2023).

³³ Peter Jeydel and Brian Egan, '[An "IEEPA-Free Zone" for TikTok and other Chinese Mobile Applications?](#)', *American Society of International Law*, 8 February 20221, Vol. 25 Issue 2.

³⁴ See: Cyber Risk GmbH, *The Restrict Act*, <https://www.restrict-act.com/> (accessed 26 July 2023).

³⁵ Johana Bhuiyan, '[Why did the US just ban TikTok from government-issued cellphones?](#)', *The Guardian*, 31 December 2022; Alex Hern, '[Canada bans TikTok on government devices over security risks](#)', *The Guardian*, 1 March 2023.

this project will not genuinely protect data from being accessed by the Chinese Communist Party (CCP).³⁶

United Kingdom

Defending Democracy Taskforce

3.46 In November 2022, the United Kingdom (UK) established the Defending Democracy Taskforce, with its primary focus being 'to protect the democratic integrity of the UK from threats of foreign interference'. Those threats were listed as:

... foreign interference in our elections and electoral processes; disinformation; physical and cyber threats to our democratic institutions and those who represent them; foreign interference in public office, political parties and universities; and transnational repression in the UK.³⁷

3.47 The taskforce reports into the UK's National Security Council.³⁸

Counter Disinformation Unit

3.48 The UK has a dedicated Counter Disinformation Unit that operates across government. Established in early 2020, its primary role at that time was to counter false COVID-19 narratives. However, it is now focused more widely on content targeted at UK audiences which poses a risk to public health, public safety, or national security, such as false COVID-19 'cures' or disinformation related to the Russian invasion of Ukraine.³⁹

UK's TikTok ban

3.49 On 16 March 2023, TikTok was banned from being installed on government devices, after Cabinet Office Ministers ordered a security review. The statement announcing the ban highlighted that:

TikTok requires users to give permission for the app to access data stored on the device, which is then collected and stored by the company. Allowing such permissions gives the company access to a range of data on the device, including contacts, user content, and geolocation data.

³⁶ Dan Milmo, '[Six urgent questions TikTok's CEO needs to answer for US lawmakers](#)', *The Guardian*, 22 March 2023.

³⁷ UK Home Office, '[Ministerial Taskforce meets to tackle state threats to UK democracy](#)', *Media release*, 28 November 2022.

³⁸ UK Government, '[Ministerial Taskforce meets to tackle state threats to UK democracy](#)', *Media release*, 28 November 2023.

³⁹ Cabinet Office (UK), *Fact Sheet on the CDU and RRU* [Rapid Response Unit], 9 June 2023, www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru (accessed 15 July 2023).

The government, along with our international partners, is concerned about the way in which this data may be used.⁴⁰

National Security Act 2023

3.50 The *National Security Act 2023* came into effect on 11 July 2023 and 'introduces new measures to modernise counter-espionage laws and address the evolving state threat to national security'. The Home Office (UK) stated:

The act introduces an offence of foreign interference, meaning it will now be illegal in the to engage in conduct that interferes with fundamental rights, such as voting and freedom of speech, that are essential to the UK's democracy.

3.51 The act also introduces a Foreign Influence Registration Scheme, similar to that operating in Australia.⁴¹

Online Safety Bill

3.52 The Online Safety Bill, which as of July 2023 is before the House of Lords, integrates closely with the *National Security Act 2023* described above. It does this by designating foreign interference offences under the National Security Act as 'priority offences' under the Online Safety Bill. The UK Government described the effect of this amendment to the Online Safety Bill on 5 July 2022:

It means social media platforms, search engines and other apps and websites allowing people to post their own content will have a legal duty to take proactive, preventative action to identify and minimise people's exposure to state-sponsored or state-linked disinformation aimed at interfering with the UK.⁴²

Canada

3.53 Electoral foreign interference, hybrid threats and cyber-enabled social media operations, including the use of cyber-attacks, have also been part of Chinese foreign interference techniques recently identified in Canada. This follows the leak in early 2023 of government intelligence documents by a whistleblower to the Globe and Mail newspaper, which reported:

Highly classified CSIS [Canadian Security Intelligence Service] documents seen by The Globe paint a picture of a broad Chinese strategy to interfere in Canada's democracy and gain influence over politicians, corporate executives, academics and vulnerable Chinese Canadians. The documents reveal that Beijing's ruling Chinese Communist Party uses three

⁴⁰ Cabinet Office (UK), '[TikTok banned on UK government devices as part of wider app review](#)', *Media release*, 16 March 2023.

⁴¹ Home Office (UK), *National Security Act 2023*, www.gov.uk/government/collections/the-national-security-bill (accessed 15 July 2023).

⁴² Department for Digital, Culture, Media and Sport UK, '[Internet safety laws strengthened to fight Russian and hostile state disinformation](#)', *Press release*, 5 July 2022; UK Parliament, *Online Safety Bill*, <https://bills.parliament.uk/bills/3137> (accessed 26 July 2023).

colour-coded 'political-interference tactics' to gain influence over Canadians here and those travelling to China.⁴³

- 3.54 The *CSIS Public Report 2021* also identifies the role cyber-attacks are playing in foreign interference campaigns, including on social media, providing an infographic and outlining that:

State-sponsored disinformation campaigns represent one of many vectors of foreign interference and hostile states have been involved in actively spreading disinformation in an effort to discredit our government institutions, negatively impact social cohesion and gain influence for their own strategic objectives.⁴⁴

Foreign Influence Registry

- 3.55 Canada has recently begun public consultation on the creation of a foreign influence registry, and in this process Australia's Foreign Influence Transparency Scheme has been included in the benchmarking that accompanied the consultation document.⁴⁵ Canada also appears to be following a similar approach to Australia and considering appointing a National Counter Foreign Interference Coordinator position within Public Safety Canada.⁴⁶

TikTok ban

- 3.56 Following a review of TikTok from the Chief Information Officer of Canada, in February 2023 the Canadian Government banned TikTok on government-issued devices. As has been the case with other jurisdictions, the public messaging in relation to the bans has been heavily framed in relation to the cyber security and privacy threat the app poses instead of foreign interference considerations.⁴⁷

New Zealand

Concern for 2023 elections

- 3.57 On 27 March 2023, media reported that 'New Zealand intelligence agencies are growing more concerned about both foreign interference and malicious cyber activity ahead of elections in October'. Phil McKee, Acting Director-General of Security, said the threat of foreign interference and espionage is a growing cause

⁴³ Steven Chase, '[A timeline of China's alleged interference in recent Canadian elections](#)', *The Globe and Mail*, 9 March 2023 (accessed 26 July 2023).

⁴⁴ Canadian Security Intelligence Service, *CSIS Public Report 2021*, March 2022, p. 18.

⁴⁵ Public Safety Canada, *Enhancing Foreign Influence Transparency: Exploring Measures to Strengthen Canada's Approach*, www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2023-nhncng-frgn-nfluence/index-en.aspx (accessed 7 July 2023)

⁴⁶ 'Ottawa considering appointing a national coordinator to counter foreign interference, minister says', *CBC News*, (accessed 7 July 2023).

⁴⁷ Alex Hern, '[Canada bans TikTok on government devices over security risks](#)', *The Guardian*, 1 March 2023.

for concern, adding information was being collected on those who speak out against foreign governments and their families being threatened in their home countries.⁴⁸

3.58 On 10 March 2023 New Zealand media reported on comments made by a member of the government's Independent Electoral Review Panel, in which it was indicated that the potential for artificial intelligence to be used to spread misinformation and disinformation in the lead-up to the October 2023 election was a topic under consideration.⁴⁹

3.59 Earlier in July 2021, statements made by the New Zealand Director-General of Security to the Justice Committee *Inquiry into the 2020 General Election and Referendums*, outlined that 'state actors pursuing their strategic goals through disinformation is an area of growing international concern' and went on to note that:

We assess that New Zealand has not been the direct target of widespread state-backed disinformation campaigns. But given the nature of global online content, members of the New Zealand public are highly likely to encounter disinformation. This means that disinformation campaigns occurring overseas may affect levels of trust in the media and government here.⁵⁰

TikTok ban on parliamentary devices

3.60 On 17 March 2023, the parliamentary service chief executive Rafael Gonzalez-Montero wrote to New Zealand MPs that the TikTok application would be banned from parliamentary work devices after determining that the 'risks are not acceptable in the current New Zealand Parliament environment'. This decision was based on the parliamentary service's analysis and discussions with colleagues across government and internationally.⁵¹

Pacific region

3.61 A recent report by the Australian Strategic Policy Institute noted that the Indo-Pacific region 'contains an arc of emergent democracies vulnerable to

⁴⁸ Lucy Craymer, '[New Zealand security chiefs increasingly concerned about foreign interference](#)', *Reuters*, 27 March 2023.

⁴⁹ Geraden Cann, '[Artificial intelligence 'likely to be used to spread disinformation' during next election](#)', *Stuff*, 10 March 2023.

⁵⁰ Director-General of Security, New Zealand Security Intelligence Service and Acting Director-General of the Government Communications Security Bureau, *Director-General remarks: Justice Committee Inquiry into the 2020 General Election and Referendums*, www.nzsis.govt.nz/news/director-general-remarks-justice-committee-inquiry-into-the-2020-general-election-and-referendums/ (accessed 7 July 2023).

⁵¹ Michael Neilson, '[TikTok app banned on phones of New Zealand MPs by Parliamentary Service amid security concerns](#)', *NZ Herald*, 17 March 2023.

coercive statecraft and foreign interference and further noted that some 'have limited civil society organisations or independent media'. The report recommended:

The US and Australian governments should invest more in fostering democratic resilience in a region that has high levels of digital penetration. Many countries in the Indo-Pacific are coming from a low base in terms of their capacity to engage with hybrid threats in the security landscape ... There's much that the US and Australia can do to build capacity and resilience among partners in the region. A construct such as a regional hybrid threats centre could provide an effective vehicle to bring together this cross-section of stakeholders—from governments, industry and civil society—to engage with the diversity of the region and the diversity of threats.⁵²

- 3.62 Dr William Stoltz of the Australian National University, also noted that work needs to be done by Australia to support countermeasures against foreign interference in the Pacific region:

... there is arguably a greater problem concerning foreign interference on social media in the countries that are closest to us and most key to our interests. This is particularly those countries in the South Pacific, where there isn't necessarily the fulsome law enforcement and digital infrastructure that we might have to provide online safety. I would say that a more urgent priority for Australia, alongside our own jurisdiction, is to be investing in the digital literacy and the infrastructure of developing countries in our region, which we know are the targets of quite comprehensive information operations by other states. Those countries, just through the underdeveloped nature of their institutions, are more vulnerable to these malicious information operations.⁵³

- 3.63 Meta advised the committee of work it is undertaking in the Pacific region, via its Pacific Islands advisory group:

[W]e've been able to develop a locally relevant digital campaign which advises and educates people across a number of different channels. It's done in a range of local languages and in ways that, hopefully, are compelling to people, to give them some tips, and in ways to provoke them to think about what they're sharing and the content they're engaging with. We've also got teams that work across the region on broader digital literacy campaigns as well.⁵⁴

International digital literacy campaigns

- 3.64 This section outlines key digital literary campaigns that have taken place abroad, many of which seek to mitigate the impact of foreign interference,

⁵² Danielle Cave and Dr Jacob Wallis, Australian Strategic Policy Institute, 'Cyber-enabled foreign interference', *Strategic Insights*, November 2022, pp. 21–22.

⁵³ Dr William Stoltz, Private capacity, *Committee Hansard*, 20 April 2023, p. 40.

⁵⁴ Ms Mia Garlick, Regional Director of Policy, Meta, *Committee Hansard*, 11 July 2023, p. 9.

misinformation and disinformation online. These campaigns could act as models for a prospective Australian public education campaign.

United States

3.65 The Federal Bureau of Investigation's Protected Voices Initiative provides information to the public on the nature of foreign cyberattacks aimed at influencing American political processes. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) have also published a range of infographics and documents aimed at raising awareness and educating individuals on how to resist foreign interference through social media.⁵⁵

3.66 In anticipation of the 2020 Presidential election, CISA launched the '#Protect2020' campaign. The campaign involved support for election officials in identifying and planning for vulnerabilities within election infrastructure.⁵⁶

United Kingdom

3.67 The UK Government has developed disinformation tools and campaigns including:

- The 'Don't Feed the Beast' campaign educates the public on the dangers of sharing inaccurate information online.
- A 'train the trainer' plan which equips teachers, library workers and carers with skills needed to assess information viewed online.
- A toolkit to help communicators manage the impact disinformation could have on their organisation.⁵⁷

European Union

3.68 The European Commission has organised a range of initiatives to increase levels of digital and media literacy, such as the 2019, *European Media Literacy Week* including 320 events across the continent and the Social Observatory for Disinformation and Social Media Analysis which 'provide strategies and actions to increase media literacy'.⁵⁸

⁵⁵ Jelisa Castrodale, '[The US Government is using pineapple pizza to explain Russian political interference](#)', *Vice*, 27 July 2019; Jacob Ward, '[U.S. cybersecurity agency uses pineapple pizza to demonstrate vulnerability to foreign influence](#)', *NBC*, 27 July 2019; Federal Bureau of Investigation, *Protected Voices: Social Media Literacy*, www.fbi.gov/video-repository/protected-voices-social-media-literacy-102319.mp4/view (accessed 3 March 2022).

⁵⁶ Law Council of Australia, *Submission 18*, p. 35.

⁵⁷ Government of the United Kingdom, *SHAREChecklist*, 2020, <https://sharechecklist.gov.uk/> (accessed 3 March 2022); Australasian Cyber Law Institute, *Submission 41*, p. 20.

⁵⁸ Law Council of Australia, *Submission 18*, p. 48.

- 3.69 As outlined earlier in this chapter, the *EUvsDisinfo* campaign aims to increase public awareness of 'disinformation operations and campaigns and increase resistance to digital information and media manipulation'.⁵⁹

Canada

- 3.70 The Canadian Government has developed the *Digital Citizen Initiative* to 'support democracy and social cohesion in Canada by building citizens' resilience against online disinformation and building partnerships to support a healthy information ecosystem'.⁶⁰

Ukraine

- 3.71 In 2015, the Ukrainian Government introduced the *Learn to Discern* program in schools to improve young people's media literacy particularly in the context of propaganda campaigns led by the Russian Government which sought to destabilise Ukrainian public institutions.⁶¹
- 3.72 The success of the program led to its adoption in other countries and some submitters recommending that Australia adopt a similar program here.⁶²

⁵⁹ Law Council of Australia, *Submission 18*, p. 46.

⁶⁰ Department of Home Affairs, *Submission 16*, p. 8.

⁶¹ Australasian Cyber Law Institute, *Submission 41*, p. 23.

⁶² See Law Society of New South Wales: Young Lawyers, *Submission 11*, p.10; and University of New South Wales Law Society, *Submission 37*, p. 28.

Chapter 4

Government: Current practice

- 4.1 In order to identify gaps in countermeasures that governments can take towards foreign interference through social media, it is vital to accurately map the steps currently being taken.
- 4.2 This chapter outlines current legislation and taskforce initiatives of the Australian Government to attempt to combat the impact of foreign interference and disinformation on social media.

Current legislative settings

- 4.3 As noted in the interim report of the Select Committee on Foreign Interference through Social Media established during the 46th Parliament (2019 select committee), while several pieces of legislation apply to social media and the online environment—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.

Criminal Code Act 1995

- 4.4 The *Criminal Code Act 1995* (Criminal Code) contains provisions that criminalise foreign interference (section 92.3).
- 4.5 These provisions were used to charge Mr Di-Sanh Duong ‘with the offence of preparing for a foreign interference offence, contrary to section 92.4 of the Criminal Code’. This matter is still before the courts.¹
- 4.6 On 14 April 2023, the Australian Federal Police (AFP) charged Mr Alexander Csergo with the offence of reckless foreign interference, contrary to section 92.3 of the Criminal Code. This matter is still before the courts.²
- 4.7 These provisions were also used in the June 2020 investigation of Mr John Zhisen Zhang, a part-time staffer of New South Wales (NSW) Labor MP Mr Shaoquett Moselmane. The AFP alleged that Mr Zhang and unnamed others used a WeChat group to advance the interests and policy goals of China by providing support and encouragement to Mr Moselmane for the advocacy of ‘Chinese state interests’ within the NSW Labor Party and to voters.
- 4.8 It was later revealed that the AFP-Australian Security Intelligence Organisation (ASIO) Foreign Interference Taskforce had also taken action in relation to

¹ Attorney-General’s Department, *Submission 25*, p. 4.

² Australian Federal Police, ‘[Australian man charged with foreign interference](#)’, *Media Release*, 14 April 2023; Echo Hui, ‘[Bondi man Alexander Csergo was warned to leave China by American contact he suspected was a spy](#)’, *ABC News*, 28 June 2023.

six Chinese citizens suspected to be part of a group of foreign agents who encouraged and helped Mr Moselmane to champion Chinese Government interests, including two academics who had their visas cancelled and four Chinese journalists who departed Australia after raids on their media outlets.³

National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018

- 4.9 The Australian Government updated the offences in the Criminal Code via the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Espionage Act) to introduce new offences relating to foreign interference with Australia's political, governmental or democratic processes. These new foreign interference offences could be applied to persons who 'weaponise' fake news in certain circumstances.⁴
- 4.10 The offences contained in the Espionage Act now extend to persons who, on behalf of a foreign government, engage in the deceptive or covert conduct intended to 'influence a political or governmental process of the Commonwealth or a State or Territory or influence the exercise (whether or not in Australia) of an Australian democratic or political right or duty'.⁵
- 4.11 At time of writing, two separate people have been charged under the Espionage Act, for actions not relating to social media. In the first case, Dr Sunny Duong is alleged to have sought to cultivate a relationship with former Coalition Minister Alan Tudge from March to June in 2020 and use that relationship to advance the interests of the Chinese Communist Party.⁶
- 4.12 The second case is that of Australian businessman Alexander Csergo, who was charged with reckless foreign interference in April 2023. Mr Csergo lived in China for decades and is alleged to have been recruited by suspected agents for China's Ministry of State Security, 'Ken' and 'Evelyn', to obtain and provide information on intelligence priorities. It is alleged they first made contact with Mr Csergo via professional networking platform, LinkedIn.⁷

³ Sean Rubinsztein-Dunlop and Echo Hui, '[Australian police accessed Chinese diplomats' emails and messages as part of foreign political interference investigation](#)', *ABC News*, 15 September 2020.

⁴ For a fulsome description of the changes that took place, see Juli Tomaras, Owen Griffiths, David Markham and Claire Petrie, [National Security Legislation Amendment \(Espionage and Foreign Interference\) Bill 2017](#), Bills Digest No 134, 2017-18, Parliamentary Library, Canberra.

⁵ *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*, s 83.4.

⁶ Hugo Timms, '[Sunny Duong: Alleged Chinese spy who donated to Liberal politician Alan Tudge faces court](#)', *News.com.au*, 28 July 2022.

⁷ Tory Shepherd, '[Vague foreign influence laws in focus as Australian businessman accused of taking money from spies](#)', *the Guardian*, 23 April 2023; and Kirsty Needham and Lewis Jackson, '[How Chinese spies allegedly tried to force Bondi man into sharing secrets about AUKUS in exchange for envelopes full of cash](#)', *Daily Mail*, 17 April 2023.

- 4.13 Both cases are still before the courts. The effectiveness of this legislation is discussed in the following Chapter 5 which discusses ideas for further government measures.

Foreign Influence Transparency Scheme Act 2018

- 4.14 The *Foreign Influence Transparency Scheme Act 2018* (Transparency scheme) is managed by the Attorney-General's Department. The scheme's stated goal is to 'provide the public with visibility of the nature, level and extent of foreign influence on Australia's government and politics', which is done via requiring individuals and entities to register certain activities under the scheme if they are taken on behalf of a foreign principal.
- 4.15 Under the Transparency scheme, a foreign principal includes a foreign government, a foreign political organisation, a foreign government related entity and a foreign government related individual. Registerable activities include parliamentary lobbying, general political lobbying, communications activities and disbursement activities (the payment of money or things of value).⁸
- 4.16 ASIO has stated the two recent changes—the Espionage Act and Transparency scheme—have assisted in the fight to counter foreign interference in Australia:

The passage of espionage and foreign interference (EFI) legislation has proven a valuable tool to ASIO and partners in preventing threats posed by foreign intelligence services (FIS) and their proxies. The legislation, coupled with operational work, caused some intelligence services to reassess the risks associated with conducting clandestine foreign intelligence operations in or against Australia, and—in some cases—they ceased activities.

We assess that the legislation also contributed to some FIS more openly declaring their intelligence presence and activities in Australia. This informed our assessments, and improved our understanding of the EFI threat in Australia, enabling us to direct our efforts towards mitigating highest harm activities.⁹

- 4.17 The Parliamentary Joint Committee on Intelligence and Security is currently undertaking a review into the operation, effectiveness and implications of the Transparency scheme which commenced on 6 February 2021.

Online Safety Act 2021

- 4.18 On 23 July 2021, the Online Safety Bill 2021 and Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021 were enacted. They retained and replicated certain provisions in the

⁸ Attorney-General's Department, *Foreign Influence Transparency Scheme*, www.ag.gov.au/integrity/foreign-influence-transparency-scheme (accessed 26 April 2023). See also Attorney General's Department, '[Foreign Influence Transparency Scheme commences today](#)', *Media Release*, 10 December 2018.

⁹ Australian Security Intelligence Organisation, *Annual Report 2019–20*, p. 42.

Enhancing Online Safety Act 2015 and made consequential amendments to 'protect more Australians from harm, or risk of harm', including through schemes regulating the non-consensual sharing of intimate images, online complaints, complaints-based removal notices and compliance requirements, and including app distribution services and internet search engine services into the remit of the new online content scheme.

- 4.19 Significantly, the amendments also gave the eSafety Commissioner (outlined in greater detail below) powers 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.¹⁰

Privacy Act 1998

- 4.20 The *Privacy Act 1988* (Privacy Act) is the principal piece of Australian legislation protecting the handling of personal information about individuals, including the collection, use, storage and disclosure of personal information in the federal public sector and in the private sector. The Attorney-General's Department is conducting a review into the Privacy Act, which is discussed in greater detail later in this chapter.

Government counter-interference entities

- 4.21 The following visualisation of the Australian Government's network for countering foreign interference maps the responsibilities and connections between departments and agencies. Further information about the participants and specific initiatives is on following pages.

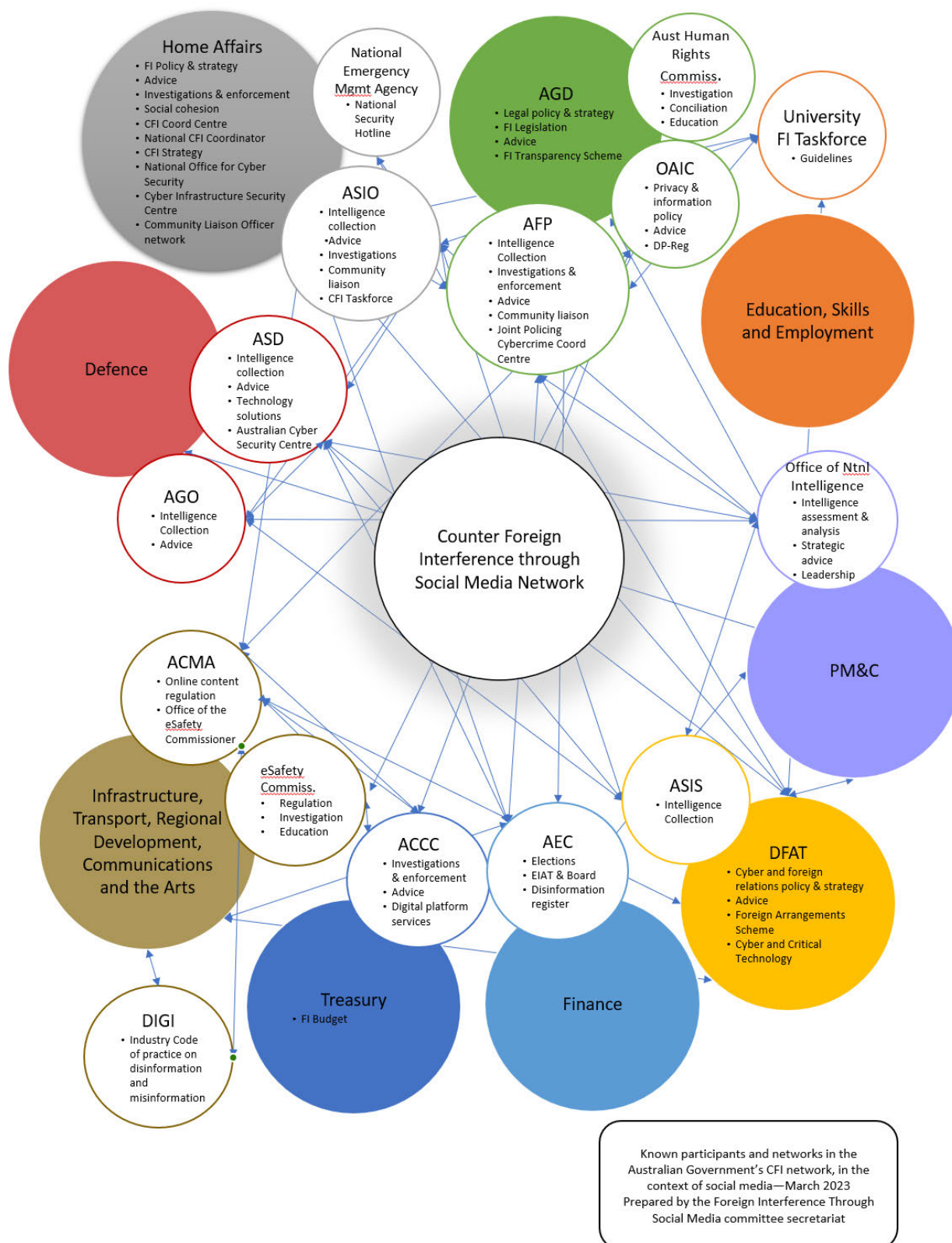
Counter Foreign Interference Strategy

- 4.22 Developed by the Department of Home Affairs (Home Affairs), the aim of the *Counter Foreign Interference Strategy* (CFI strategy) is to protect Australia's sovereignty, values and national interests from foreign interference. The CFI strategy includes five pillars aimed at enhancing capability, engaging with at-risk sectors, deterring perpetrators, defending against acts of foreign interference, and enforcing counter foreign interference laws.¹¹ A summary of the CFI strategy is published on the Home Affairs website, but further details are not publicly available.

¹⁰ The Hon Paul Fletcher MP, Minister for Communications, Urban Infrastructure, Cities and the Arts, *House of Representatives Hansard*, 24 February 2021, p. 1785.

¹¹ Department of Home Affairs, *Australia's Counter Foreign Interference Strategy*, www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-strategy (accessed 17 February 2023).

Figure 4.1 Counter foreign interference network



Home Affairs

- 4.23 As well as participating in taskforces and other initiatives described below, Home Affairs advised the committee of broader activities it undertakes in relation to foreign interference.
- 4.24 Home Affairs submitted that it engages ‘with a range of international partners through a variety of bilateral and multilateral forums to share information and exchange policy best practice approaches to counter foreign interference and malign information activities’. Home Affairs further submitted that this engagement ‘informs Australia’s domestic policies and legislative frameworks to protect Australian interests from hostile state actor activities’.¹² However, no specific information was given on which international fora it participates in, nor which specific policies were adopted from overseas best practice.
- 4.25 Home Affairs noted that it uses an integrated model to counter misinformation and disinformation online, particularly promoting Australian values and Australia’s inclusive national identity, but gain, did not provide anything specific as to whether it follows similar counter-tactics as outlined in Chapter 3 on international approaches, such as using the DISARM or other agreed frameworks.¹³

National Counter Foreign Interference Coordinator

- 4.26 The inaugural National Counter Foreign Interference Coordinator (NCFIC), Mr Chris Teal, was appointed in 2018 to work across government and non-government sectors to strengthen arrangements to counter foreign interference. The NCFIC administers the CFI strategy and is supported by the Counter Foreign Interference Coordination Centre (CFICC).¹⁴

Counter Foreign Interference Coordination Centre

- 4.27 The Home Affairs CFICC coordinates all Australian Government responses to foreign interference, including through the CFI strategy, outreach efforts and advice, engagement with culturally and linguistically diverse (CALD) communities, and engagement with international and regional partners.¹⁵
- 4.28 CFICC Partnership teams located in all states and territories also work closely with communities, state/territory governments, police and national security

¹² Department of Home Affairs, *Submission 1*, p. 4.

¹³ Department of Home Affairs, *Submission 1*, p. 4.

¹⁴ Department of Home Affairs, *National Counter Foreign Interference Coordinator*, www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-coordinator (accessed 17 February 2023).

¹⁵ Department of Home Affairs, *Countering foreign interference*, www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference (accessed 18 January 2023).

agencies to build community awareness of, and resilience to, the threat of foreign interference.¹⁶

Counter Foreign Interference Taskforce

- 4.29 Established in 2020 and lead by ASIO, the CFI Taskforce, discovers, disrupts and investigates foreign interference activity, including through investigations and enforcement activity. Membership includes ASIO, Home Affairs and the AFP.¹⁷ ASIO noted that the taskforce is ‘designed to mitigate harm and disrupt the threat of espionage and foreign interference by leveraging the unique capabilities of our intelligence and law enforcement agencies and it uses a range of mechanisms such as ‘intelligence operations, law enforcement activity and prosecutions under the Espionage and Foreign Interference Legislation and the Foreign Influence Transparency Scheme, visa cancellations, and financial disruptions’.¹⁸
- 4.30 The CFICC confirmed with the committee that it is not a member of the CFI Taskforce because ‘structure is an operational activity, and Home Affairs does not undertake the operational investigative aspects’ however it was noted that the CFICC has ‘responsibility for the oversight board for the taskforce and engage[s] with them to inform policy and to work with them on policy aspects of investigations’.¹⁹

Australian Cyber Security Centre

- 4.31 The Australian Cyber Security Centre leads the Australian Government's efforts to improve cyber security by providing advice, alerts and information about cyber threats and monitoring threats globally and developing solutions, including in relation to foreign interference and disinformation. The Australian Government has committed to 10 years of investment in the Australian Signals Directorate (ASD)—known as REDSPICE—to improve cyber defences from 2022–23.²⁰

¹⁶ Department of Home Affairs, *Countering foreign interference in communities*, www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/in-communities (accessed 21 February 2023); Senate Standing References Committee on Foreign Affairs, Defence and Trade, *Human rights implications of recent violence in Iran final report*, February 2023, p. 47.

¹⁷ Department of Home Affairs, *Countering foreign interference*.

¹⁸ Australian Security Intelligence Organisation, *Submission 2*, p. 6.

¹⁹ Ms Sally Pfeiffer, Acting First Assistant Secretary, Counter Foreign Interference, Department of Home Affairs, *Committee Hansard*, 12 July 2023, p. 12.

²⁰ Australian Cyber Security Centre, Australian Signals Directorate, *Annual cyber threat report July 2021–June 2022*, p. 11.

Cyber and Infrastructure Security Centre

- 4.32 The Cyber and Infrastructure Security Centre of Home Affairs actively assists Australian critical infrastructure owners and operators to understand the risk environment and meet their cyber-related regulatory requirements, in addition to its own regulatory requirements. It works in partnership with government, industry and community.

Foreign Influence Transparency Scheme

- 4.33 The Foreign Influence Transparency Scheme commenced on 10 December 2018. The purpose of the scheme is to provide the public with visibility of the nature, level and extent of foreign influence (rather than interference) on Australia's government and politics, including through registration of individuals and entities, foreign principals, and registerable activities, with additional obligations during voting periods.²¹
- 4.34 Under the scheme, communications activities such as those conducted on social media need to be registered if they are undertaken in Australia on behalf of a foreign principal for the purpose of political or government influence. The Attorney-General's Department advised that all scheme registrants met their obligations under the act in relation to the 2022 federal election.

Community Liaison Officer network

- 4.35 The Home Affairs network of Regional Directors and Community Liaison Officers engage with a wide range of cultural, religious and ethnic community stakeholders around Australia, to 'support the communication of official information to CALD communities, and provides a mechanism for community members to share information about their priorities, concerns, and the impact of government policies and programs on their communities'.²²

National Security Hotline

- 4.36 The National Security Hotline, administered by the National Emergency Management Agency, takes reports of suspicious behaviour in relation to terrorism and foreign interference, including where people are 'being intimidated or harassed by someone linked to a foreign government' or 'coerced to return to their home country'.²³

²¹ Attorney-General's Department, *Foreign Influence Transparency Scheme*, www.ag.gov.au/integrity/foreign-influence-transparency-scheme (accessed 17 February 2023); Attorney-General's Department, *Submission 13: Foreign Interference through Social Media inquiry* (46th Parliament), p. 9.

²² Attorney-General's Department, *Submission 13: Foreign Interference through Social Media inquiry* (46th Parliament), p. 8.

²³ Australian Government, *Australian National Security: report suspicious behaviour*, www.nationalsecurity.gov.au/what-can-i-do/report-suspicious-behaviour, (accessed 16 February 2023).

University Foreign Interference Taskforce

- 4.37 The University Foreign Interference Taskforce (UFIT) was established in 2019, to support and build resilience against foreign interference in universities. The UFIT Steering Group 'primary conduit for all university and Government counter foreign interference related activities'. In 2019, UFIT released the Guidelines to Counter Foreign Interference in the Australian University Sector, with an update released in November 2021.²⁴
- 4.38 Evidence received during the *Inquiry into national security risks affecting the Australian higher education and research sector* suggested that the taskforce is unique amongst Five Eyes Plus nations, and that it has been a highly successful collaborative approach which has been mirrored in other jurisdictions.²⁵

Strengthening Democracy Taskforce

- 4.39 Announced on 8 December 2022, the Strengthening Democracy Taskforce, housed within Home Affairs, aims to bolster Australia's democratic resilience and enhance trust among citizens, and between citizens and governments. The taskforce will work in partnership with Australian civil society organisations to deliver a practical agenda for sustaining and strengthening our democratic resilience. The taskforce will work closely with the newly established National Resilience Taskforce 'noting Australia's democratic resilience underpins our national resilience'.²⁶

Election Integrity Taskforce

- 4.40 The Election Integrity Taskforce is comprised of a range of Australian Government agencies who provide specialist support to the Australian Electoral Commission (AEC) to support election integrity including cyber security and disinformation. The taskforce supports various electoral events, including federal by-elections and State and territory elections. The AEC submitted that 'Taskforce agencies did not identify any foreign interference, or any other interference, that compromised the delivery of the 2022 federal election'.²⁷
- 4.41 However, David Robinson of Internet 2.0 expressed scepticism on this. He pointed to a study of social media commentary after the 2021 coup in Myanmar, where the Pentagon's social media accounts were hit with 700 000

²⁴ Department of Education, University Foreign Interference Taskforce, [Guidelines to Counter Foreign Interference in the Australian University Sector](#), 17 November 2021.

²⁵ Joint Standing Committee on Intelligence and Security, [Inquiry into national security risks affecting the Australian higher education and research sector](#), March 2022, pp. 89–93 and 105–106.

²⁶ Department of Home Affairs, *Submission 1*, p. 5. See also The Hon Clare O'Neil MP, Minister For Home Affairs, [Strengthening democracy taskforce](#), 8 December 2022.

²⁷ Australian Electoral Commission, *Submission 8*, p. 2.

posts related to the coup. Social media companies and providers tracked the authenticity of the debate and found that it was authentic behaviour. However, when Internet 2.0 studied the data from a mathematical analysis perspective, they were easily able to identify an inauthentic campaign. In relation to the safety of Australian elections from CIB, Mr Robinson stated that until someone had done similar analysis 'I don't think you can say either way'.²⁸

Code of practice on misinformation and disinformation

4.42 In December 2019, the Australian Government requested that major digital platforms in Australia develop a voluntary code of practice to address online disinformation and news quality concerns.

4.43 In February 2021, Digital Industry Group Inc (DIGI) published the *Australian Code of Practice on Disinformation and Misinformation* (DIGI code) with 8 signatories: Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitter. The DIGI code aimed to provide safeguards against harms from the spread of mis and disinformation on digital platforms. The DIGI code was then updated in October 2022 with changes to the code's governance.²⁹

4.44 The objectives of the DIGI code are:

- (a) Provide safeguards against harms that arise from mis and disinformation.
- (b) Disrupt advertising and monetisation incentives for mis and disinformation.
- (c) Work to ensure the integrity and security of services and products delivered by digital platforms.
- (d) Empower consumers to make better informed choices of digital content.
- (e) Improve public awareness of the source of political advertising carried on digital platforms.
- (f) Strengthen public understanding of mis and disinformation through support of strategic research.
- (g) Signatories publicise measures they take to combat mis and disinformation.³⁰

Australian Communications and Media Authority

4.45 The Australian Communications and Media Authority (ACMA) is the independent statutory authority responsible for the regulation of broadcasting, radiocommunications and telecommunications in Australia. The ACMA's remit

²⁸ Mr David Robinson, Director, Internet 2.0, Committee Hansard, 20 April 2023, p. 36. The AEC was not asked by the committee whether it had conducted a similar mathematical analysis.

²⁹ Digital Industry Group Inc, [Australian Code of Practice on Disinformation and Misinformation](#), 22 February 2021 and Digital Industry Group Inc, [Australian Code of Practice on Disinformation and Misinformation](#), updated 11 October 2021.

³⁰ Digital Industry Group Inc, *Australian Code of Practice on Disinformation and Misinformation*, updated 11 October 2021, pp. 10–15.

also includes aspects of online content regulation; relevantly, the ACMA monitors digital platforms' activities under the DIGI code, including in response to coordinated campaigns by foreign actors.³¹

- 4.46 In June 2021, the ACMA finalised *A report to government on the adequacy of digital platforms' disinformation and news quality measures*. The ACMA found the scope of the DIGI code is limited by the threshold where both 'serious' and 'imminent' harm must be reached before action is required. 'The effect of this is that signatories could comply with the code without having to take any action on the type of information which can, over time, contribute to a range of chronic harms, such as reductions in community cohesion and a lessening of trust in public institutions.'³² The DIGI code was subsequently updated by signatories, to change the definition of harm to a threshold of 'serious and credible' threat of harm.³³
- 4.47 The ACMA found challenges in obtaining relevant data on platform actions in Australia and recommended:
- That the ACMA be vested with formal information-gathering powers (including powers to make record-keeping rules) to incentivise greater platform transparency and improve access to data on the effectiveness of measures to address mis and disinformation in Australia.
 - The ACMA be vested with reserve regulatory powers in relation to digital platforms – such as code registration powers and the ability to set standards.
 - A misinformation and disinformation Action Group be established to support collaboration and information-sharing between digital platforms, government agencies, researchers and non-government organisations on issues relating to mis and disinformation.³⁴
- 4.48 The Australian Human Rights Commission (AHRC) also noted that although platforms are publishing transparency reports under the DIGI code, and the code itself was updated in December 2022, 'none of these existing measures are specifically focused on the question of foreign interference through social media, or the particular strategic risks posed to Australia through these activities'.³⁵

³¹ Australian Communications and Media Authority, *Submission 6*, p. 1.

³² Australian Communications and Media Authority, [*A report to government on the adequacy of digital platforms' disinformation and news quality measures*](#) (Report on digital platform measures), p. 3.

³³ Digital Industry Group Inc, *Submission 36*, p. 4.

³⁴ Australian Communications and Media Authority, *Report on digital platform measures*, p. 4–5.

³⁵ Australian Human Rights Commission, *Submission 9*, p. 7.

- 4.49 On 21 March 2022 the Australian Government announced it would consult on proposals to introduce legislation in the second half of 2022 to combat harmful online mis and disinformation.³⁶ These new powers for the ACMA have been proposed via an exposure draft of new legislation, which is discussed in greater detail later in this chapter.

eSafety Commissioner

- 4.50 The eSafety Commissioner is Australia's independent regulator for online safety with a role to help safeguard Australians at risk from online harms and to promote safer, more positive online experiences. While foreign interference is not a matter which falls directly within the remit of the eSafety Commissioner, this activity intersects with two of its functions, namely its role in promoting 'Safety by Design' principles and compliance with the government's 'Basic Online Safety Expectations'.³⁷

DP-REG

- 4.51 The Digital Platform Regulators Forum (DP-REG) was established in early 2022 to facilitate better coordination across government on digital platform regulation. It includes the ACMA, the Australian Competition and Consumer Commission, the Office of the eSafety Commissioner, and the Office of the Australian Information Commissioner.
- 4.52 DP-REG's strategic priorities for 2022–23 include a focus on the impact of algorithms, efforts to improve transparency of digital platforms' activities and how they are protecting users from potential harm—including from mis and disinformation—and increased collaboration and capacity building between members.³⁸

Recent policy responses and initiatives

Budget 2023–24

- 4.53 On 9 May 2023, the Australian Government announced a range of measures to improve privacy, digital safety, cybersecurity and development of critical technology industries. There were a number of key budget which are likely to directly impact on matters relating to foreign interference through social media, including:
- funding to progress the government's response to the Privacy Act review (\$0.9 million over two years);

³⁶ Department of Infrastructure, Transport, Regional Development, Communications and the Arts, [Media release: New disinformation laws](#), 21 March 2022.

³⁷ eSafety Commissioner, *Submission 10*, p. 1.

³⁸ Australian Communications and Media Authority, *Submission 6*, p. 4.

- funding to help combat scams and mis and disinformation, including:
 - funding for the ACMA to resource the Office of the eSafety Commissioner—\$134.1 million over four years (\$33.7 million per year ongoing, in addition to the existing base funding of \$10.3 million per annum ongoing). This will be partly met by existing departmental resourcing and be used for a variety of programs including 'enhanced educational, outreach and investigatory activities';
 - funding for the ACMA for the implementation of 'new powers to hold digital platforms to account and improve efforts to combat harmful misinformation and disinformation in Australia'—\$7.9 million over four years;
- establishment of the Coordinator for Cyber Security within Home Affairs—\$46.6 million over four years, then \$11.8 million per year ongoing. Noting this appears to be funding redirected from ASD rather than new funding; and
- support for local news and media and promotion of media literacy, including \$2.5 million over two years 'to build media literacy in culturally and linguistically diverse communities. This funding will be used by the government to:
 - ... partner with the Federation of Ethnic Communities' Council of Australia (FECCA) to support media literacy in culturally and linguistically diverse (CALD) communities. This partnership aims to empower multicultural communities to combat harms associated with the proliferation of deceptive information including mis and disinformation, and support improved economic and civic participation.³⁹

Privacy Act amendments and review

4.54 The first interim report of the 46th Parliament inquiry into foreign interference discussed potential amendments to the Privacy Act, including the 'introduction of a binding online privacy code for social media and certain other online platforms'.⁴⁰ However, ultimately the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 passed into law on 12 December 2022 without introducing such a requirement.⁴¹ Rather, the bill increased penalties for serious or repeated interferences with privacy, enhanced enforcement powers for the Australian Information Commissioner, and

³⁹ Australian Government, *Budget 2023–24: Budget Measures*, [Budget Paper No. 2](#), p. 183; The Hon Michelle Rowland MP, Minister for Communications, ['Budget 2023-24: Connecting, informing and protecting Australians'](#), Media release, 9 May 2023.

⁴⁰ Attorney-General's Department, [Online Privacy Bill Exposure Draft](#).

⁴¹ Parliament of Australia, [Privacy Legislation Amendment \(Enforcement and Other Measures\) Bill 2022](#).

provided the commissioner and the ACMA with greater information sharing powers.⁴²

- 4.55 In 2020, following the initial Australian Competition and Consumer Commission digital platforms inquiry of 2019, the Attorney-General commenced a review of the Privacy Act, releasing a review report in February 2023.⁴³
- 4.56 Reforms proposed by the report include stronger protections for personal information, greater transparency and control for individuals over their information, and more enforcement and redress mechanisms.⁴⁴ The Attorney-General's Department informed the committee that 'the general theme around the review itself was to conduct an uplift in terms of individuals' control over their personal data and how it's used, and also generally awareness raising and transparency initiatives'.⁴⁵
- 4.57 The report included discussion about the scope for political disinformation in relation to political targeting and microtargeting, including the 'involvement of foreign interests in political communication' and the possibility of negative impacts on democracy. Many submitters to the review referenced the Cambridge Analytica matter and 'expressed concern about whether the political exemption may allow such an incident in Australia'.⁴⁶
- 4.58 Discussion also considered the security of personal information held by political parties and the potential for this information to be targeted by foreign interference in elections, with the proposal that political entities be required to take 'reasonable steps to protect personal information'.⁴⁷
- 4.59 Disinformation was also considered in the report the context of direct and targeted marketing and serious negative impacts which this can cause, 'for example by contributing to disinformation campaigns or by discriminating against certain groups' and 'risks undermining other public interests, including the integrity of the democratic electoral process'.⁴⁸

⁴² *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 Explanatory Memorandum*, 2022, p. 2; Attorney-General's Department, *Submission 25*, p. 7.

⁴³ Attorney-General's Department, *Privacy*, www.ag.gov.au/rights-and-protections/privacy (accessed 17 July 2023); Attorney-General's Department, [Privacy Act Review — Report on a page](#).

⁴⁴ Attorney-General's Department, [Privacy Act Review Report 2022](#), pp. 5, 7 and 12–14; Attorney-General's Department, *Submission 25*, p. 8.

⁴⁵ Ms Sarah Chidgey, Deputy Secretary, National Security and Criminal Justice, Attorney-General's Department, *Committee Hansard*, 12 July 2023, p. 22.

⁴⁶ Attorney-General's Department, *Privacy Act Review Report 2022*, pp. 75–81.

⁴⁷ Attorney-General's Department, *Privacy Act Review Report 2022*, pp. 82–83.

⁴⁸ Attorney-General's Department, *Privacy Act Review Report 2022*, pp. 200 and 210.

- 4.60 The review report also examined international data flows, specifically mentioning concerns raised in relation to social media platform TikTok. The report considered options for regulating privacy for foreign organisations or small business operations which have an 'Australian link' and allowing for the flow of information overseas while ensuring privacy is protected including the Cross-Border Privacy Rules or a domestic certification scheme. However, the report noted that some 'submissions noted that personal information transferred overseas could potentially be accessed by overseas governments, and that it could be more difficult for individuals to enforce privacy rights and access justice for overseas privacy infringements'.⁴⁹
- 4.61 The Attorney-General's Department sought feedback by 31 March 2023 to its review report, noting that feedback would 'inform the Australian Government's response to this report to ensure that any reforms the Australian Government implements are balanced and effective'. There is no information available on any timeline for proposed changes to the Privacy Act.⁵⁰
- 4.62 However, the United States Federal Communications Commissioner, Mr Brendan Carr, expressed some doubt that privacy protections would be wholly effective. Commissioner Carr noted that Europe has 'gold standard' privacy protections, but is still finding it necessary to ban apps such as TikTok:

If privacy protections were enough to address TikTok then we wouldn't see these concerns existing today in Europe. So privacy is important, but, when we're dealing with a company with a history of misrepresentations, because of their conduct, we do not have a baseline level of trust. Privacy protection isn't tailored to address those national security threats.⁵¹

AEC activities

- 4.63 As noted above, the AEC is a member of the Election Integrity Taskforce and has undertaken a number of activities designed to protect election-related activity in Australia. However, the AEC noted that while the *Electoral Act 1918* does 'require electoral matter to be properly authorised to inform voters of the source of communication' it 'does not regulate truth in electoral communication'.⁵² In other words, a person or organisation can provide false information, but they must put their name to it.
- 4.64 The AEC noted that as part of its integrity work, it has launched a 'purpose-built Command Centre for rapid and coordinated incident response, including a

⁴⁹ Attorney-General's Department, *Privacy Act Review Report 2022*, pp. 242 and 247–248.

⁵⁰ Attorney-General's Department, *Government response to the Privacy Act Review Report*, <https://consultations.ag.gov.au/integrity/privacy-act-review-report/> (accessed 17 July 2023).

⁵¹ Mr Brendan Carr, Commissioner, United States Federal Communications Commission, *Committee Hansard*, 20 April 2023, p. 8.

⁵² Australian Electoral Commission, *Submission 8*, p. 2.

dedicated media hub to quickly respond to electoral disinformation’ as well as a ‘Disinformation Register to list and debunk electoral process disinformation’. The AEC further noted it has developed effective working relationships with social media organisations, including a signed public agreement with Meta, Twitter, Google, Microsoft and TikTok.⁵³ However, CyberCX expressed doubt that any department or agency ‘has the capability or authority to lead in relation to a social media disinformation campaign related to political parties, candidates or policies’.⁵⁴

- 4.65 Dr Andrew Dowse of RAND Australia noted that an unintended consequence of election blackout periods for mainstream media, was that it drove people to social media where there was less chance of appropriately moderated information, and this should be considered.⁵⁵

Stop and consider campaign

- 4.66 The AEC managed the *Stop and Consider* campaign during the 2022 federal election to help voters to cut through disinformation and spin messages they may receive.
- 4.67 Information was distributed to voters primarily via social media feeds and through digital displays with translated material distributed through CALD audiences. The AEC also operated a disinformation register listing prominent pieces of disinformation regarding the election process.⁵⁶
- 4.68 Chapter 7 contains more in-depth discussion around these education and digital literacy campaigns run by the AEC and other entities.

Voice referendum

- 4.69 The AEC has also noted work being done on the proposed referendum to be held later in 2023, to help prevent the spread of disinformation. The AEC noted that due to the long time since the last referendum in 1999, there are approximately 7.4 million people who will never have voted in a referendum before and this lack of experience ‘coupled with the ever-increasing digital consumption of information, means social media platforms will undoubtedly play a key role for electors seeking information’.⁵⁷

⁵³ Australian Electoral Commission, *Submission 8*, pp. 2–3.

⁵⁴ CyberCX, *Submission 16*, p. 7.

⁵⁵ Dr Andrew Dowse, Director, RAND Australia, *Committee Hansard*, 20 April 2023, p. 29.

⁵⁶ Australian Electoral Commission, ‘[AEC launches campaign to combat disinformation](#)’, *Media release*, 12 April 2022.

⁵⁷ Australian Electoral Commission, *Submission 8*, p. 1.

Home Affairs review of foreign interference through social media

- 4.70 Home Affairs was tasked by the Home Affairs Minister in September 2022, with undertaking a review into Foreign Interference through Social Media Applications. The review was asked to consider all options to address data security risks, as well as disinformation concerns as they relate to social media platforms and was delivered to the Minister for Home Affairs on 16 March 2023 and is not expected to be publicly released.⁵⁸
- 4.71 CyberCX noted that this review was expected to look at data harvesting by TikTok and other social media platforms, but noted it is unclear whether platforms' content moderation and algorithm practices were also reviewed.⁵⁹

TikTok on Australian Government devices

- 4.72 Following the delivery of the Home Affairs review outlined above, on 4 April 2023. TikTok was banned from on devices issued by Australian Government departments and agencies. The ban is discussed in greater detail in Chapter 6.

Community outreach

- 4.73 On 14 February 2023, the Minister for Home Affairs announced a new community outreach program to be coordinated by Home Affairs and ASIO. The program will identify individuals within the Australian community who might be targets of foreign interference and design and deliver a program to proactively help them understand what foreign interference is, how they can respond, and what the government can do to protect them.⁶⁰
- 4.74 Home Affairs advised the committee on 12 July 2023, that this program has begun and is 'looking to identify communities that we think are at risk and to then proactively engage with them and seek opportunities to provide them information and make sure that we're engaging in understanding their concerns'. Home Affairs advised it had not been allocated any new resources for this program, which it had already been undertaking, simply not at this scale.⁶¹
- 4.75 On 27 February 2023, the AFP announced the launch of an education campaign to help CALD communities understand what foreign interference is, how it manifests itself and where victims can report instances and seek assistance.

⁵⁸ Department of Home Affairs, *Submission 1*, p. 5 and Mr Peter Anstee, Acting First Assistant Secretary, Department of Home Affairs, *Committee Hansard*, 12 July 2023, p. 2.

⁵⁹ CyberCX, *Submission 16*, p. 7.

⁶⁰ The Hon Clare O'Neil MP, Minister for Home Affairs, [*Minister for Home Affairs, Foreign interference in Australia - ANU address*](#), 14 February 2023.

⁶¹ Ms Sally Pfeiffer, Department of Home Affairs, *Committee Hansard*, 12 July 2023, p. 13.

It will include meetings between AFP community liaison teams, CALD groups and religious leaders, and a factsheet translated into more than 30 languages.⁶²

National Office for Cyber Security

4.76 On 27 February 2023, the Prime Minister and the Minister for Home Affairs jointly announced the creation of a new National Office for Cyber Security, to help mitigate the impact of major cyber incidents. The office will help establish a strategic and structured approach to cyber security across government, and help to manage cyber incidents in a seamless and strategic way across government. The Australian Government is also proposing a discussion paper to improve the function of relevant laws and policies.⁶³

Data Security Action Plan

4.77 Under current development, Australia's first *Data Security Action Plan* is a key initiative under the *Cyber Security Strategy 2023-2030*, that will seek to strengthen data security policy settings across government and the broader economy, including consideration of storage settings of domestic and international data and whether they adequately promote privacy, security and transparency.⁶⁴

4.78 From 6 April to 24 June 2022, Home Affairs undertook consultation and received 81 submissions on the plan. As of 10 July 2023, Home Affairs is currently developing the final plan.⁶⁵

⁶² Australian Federal Police, '[AFP launches new resource to help combat foreign interference](#)', *Media release*, 27 February 2023.

⁶³ CyberSecurity Connect, '[Federal government to stand up new National Office for Cyber Security](#)', 27 February 2023.

⁶⁴ Department of Home Affairs, *Submission 1*, p. 5.

⁶⁵ Department of Home Affairs, *Uplifting data security across Australia*, www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/data-security (accessed 10 July 2023).

Chapter 5

Government: ideas for action

- 5.1 The Australian Security Intelligence Organisation (ASIO) described the threat of foreign interference as being at the highest level in Australia's history.¹
- 5.2 Throughout this inquiry, the Select Committee on Foreign Interference through Social Media (committee) received advice from expert organisations, members of the community, government agencies and the platforms themselves on steps which are urgently required to improve the countermeasures taken against foreign interference through social media, and to protect Australia's democratic resilience.
- 5.3 A key theme emerged among the recommendations: the need for cross-sector, cross-border alliances, where government, platforms and civil society work together to tackle the threat of foreign interference. These recommendations are discussed in the next three chapters. While recognising the inter-connectedness of many of these recommendations, they have been broken down by who would be the lead entity for each recommendation: government, platforms or civil society. This chapter will outline proposals for action where government would be either the sole, or lead entity.
- 5.4 The committee heard a common message from a range of experts and people from impacted communities consistently confirming that not enough was being done by government to address foreign interference and coordinated inauthentic behaviour (CIB) through social media.
- 5.5 CyberCX submitted a range of recommendations and noted that it believes the Australian Government's responses have not kept pace with the nature and scale of the risks of foreign interference through social media.²
- 5.6 The Australian Strategic Policy Institute (ASPI) made a similar overall observation, and advised:

Today, our key recommendation for the Australian government is it needs to lead on the issue and not rely on social media platforms and civil society fact checkers to counter disinformation. This includes incorporating counter foreign interference through social media into a broader national security strategy and mandating platforms to disclose covert state backed influence operations...The ongoing issue of foreign interference through social media

¹ Lisa Visentin and Matthew Knott, ["It feels like hand-to-hand combat": ASIO boss warns on spy hives, foreign interference'](#), *Sydney Morning Herald*, 21 February 2023.

² CyberCX, *Submission 16*, p. 7.

requires a whole-of-government and proactive strategy to protect the integrity of our democracy and the wellbeing of our citizens.³

Lead agency

- 5.7 There have long been concerns expressed by the private sector expert community on the ‘lack of clarity on which parts of the Australian Government have leadership and authority in protecting which parts of Australia’s information environment—the public sector, the private sector and individual citizens—from interference by foreign actors acting with malicious intent’.⁴
- 5.8 These concerns were repeated by many submitters and witnesses, who noted that although there were numerous specialist taskforces (outlined in Chapter 4), a single lead agency to take core responsibility is needed, while ensuring appropriate coordination and collaboration with other agencies, platforms and private sector experts.
- 5.9 Indeed, the previous report of this committee also identified the absence of a single, lead focal point for cyber-enabled foreign interference. This problem has been a long-standing one, across multiple governments. It should be noted that submitters acknowledge a need for a whole of government approach, not replacement of such an approach with one lead agency.
- 5.10 CyberCX recommended:
- A single lead entity is needed to coordinate government policy and action on cyber-enabled interference. Importantly, it will also create a clear ‘one-stop-shop’ for citizens and private sector stakeholders to report, and seek advice about, foreign interference risk linked to social media.⁵
- 5.11 ASPI also recommended the government take a stronger lead on this issue:
- ...to ensure clarity on which government institutions are responsible for dealing with cyber-enabled foreign interference from both an operational and policy perspective. Currently, uncertainty as to whom in government has responsibility is creating a disincentive for victims to report while not providing disincentives to perpetrators to cease their malicious activity.⁶
- 5.12 ASPI further recommended that ‘cyber-enabled foreign interference should be incorporated into broader cybersecurity and national security strategies’.⁷

³ Mr Albert Zhang, Analyst, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 18.

⁴ Danielle Cave and Dr Jacob Wallis, ‘[AUSMIN 2022: Cyber-enabled foreign interference](#)’, *The Strategist*, 1 December 2022.

⁵ CyberCX, *Submission 16*, p. 7.

⁶ Australian Strategic Policy Institute, *Submission 13*, p. 12. See also: Mr Albert Zhang, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 21.

⁷ Australian Strategic Policy Institute, *Submission 13*, p. 12.

5.13 The Australian Human Rights Commission (AHRC) noted:

In order to address this specific risk, the Australian Government should establish a permanent whole-of-government taskforce dedicated to preventing and combating cyber-manipulation in Australia. The terms of reference for this taskforce should extend beyond those of the Electoral Integrity Assistance Taskforce to encompass not solely threats to the integrity of a federal election or electoral integrity, but threats to Australia's democracy more broadly.⁸

5.14 A joint submission from technical specialist University centres noted the complexity of the many varied government agencies and taskforces which have roles in this space, and noted that:

...it is unclear what exactly each governmental body's role is and whether foreign interference on social media falls within each body's scope of concern. Moreover, there is often little information about how much progress these various governmental bodies have made in monitoring or mitigating disinformation. Compounding this complexity, there does not appear to be a single body responsible for coordinating the government's response to the risks posed to democracy online (whether it be through disinformation or other phenomena on social media and the internet more broadly). Nor is there a single point of contact for the public regarding these risks.⁹

Standards-based regulation

5.15 The inquiry dove deeply into the issue of whether government should address the risks posed by specific platforms and applications by banning them, or whether a platform neutral approach should be taken to set standards that all platforms should meet. However, the committee noted there is a clear distinction between platforms which originate in authoritarian states rather than liberal democracies, with a specific set of risks attached, and that risk is discussed in the following chapter on platforms.¹⁰

5.16 More than one witness described the approach of banning specific platforms as 'whack a mole', where dealing with risks platform by platform simply meant a new one would pop up to replace each banned platform.

5.17 ASPI advised that an approach to use legislated standards rather than bans on individual applications was preferable but noted that 'there's also a need for bespoke legislation that accepts the fact that there is a unique problem with

⁸ Australian Human Rights Commission, *Submission 9*, p. 8.

⁹ UNSW Allens Hub for Technology, Law and Innovation, Society on Social Implications of Technology and Deakin University Centre for Cyber Security Research and Innovation, *Submission 19*, p. 5.

¹⁰ See: Dr William Stoltz, Private capacity, *Committee Hansard*, 20 April 2023, p. 38; Ms Lindsay Gorman, Senior Fellow for Emerging Technologies, Alliance for Securing Democracy, German Marshall Fund, *Committee Hansard*, 21 April 2023, p. 10.

social media apps that come from authoritarian countries' and pointed to the United States RESTRICT Act as a step in the right direction.¹¹

- 5.18 Ms Lindsay Gorman of the Alliance for Security Democracy also recommended an approach which outlines the safety standards expected of platforms and apps, but that also takes into account the additional risks inherent in apps based within authoritarian states:

My first recommendation was to come up with this overarching framework that includes the threat of platforms from authoritarian regimes and really spells out what the concerns are. Is it scale? Is it the degree of ownership and influence? Is it the type of platform itself? ... I think there needs to be a much broader framework and a much clearer framework so that when authoritarian internet apps do come to democracies, as they inevitably will in open societies, we have a framework for addressing it, and we don't have to wait until it becomes this behemoth of an issue to deal with a specific platform.¹²

- 5.19 Ms Gorman pointed to the Prague proposals on 5G internet as a 'fantastic starting point for this kind of legislative development which does identify countries of origin while also trying to promote standards that apply to any internet platform'.¹³
- 5.20 Ms Gorman further advised for separate regulation on AI generated content, because the 'democratisation of the ability to create extremely realistic but completely fake content... increases avenues for propaganda [that is] designed to spoof and generate content that looks plausible, and sounds like it might be written by a human, but isn't necessarily true'. Ms Gorman expressed concern that 'our knowledge base of what is actually true becomes at risk and our very trust in information becomes downgraded'.¹⁴
- 5.21 For example, Ms Gorman pointed to existing content authenticity frameworks such as watermarks, which could be mandated 'so you can tell when an image has been manipulated and when it hasn't, and you can track the history of that image'.¹⁵
- 5.22 The AHRC recommended the Australian Government 'introduce transparent user-data privacy and user-data protection frameworks that apply to all social

¹¹ Mr Fergus Ryan, Analyst, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 21.

¹² Ms Lindsay Gorman, Alliance for Securing Democracy, *Committee Hansard*, 21 April 2023, p. 10.

¹³ Ms Lindsay Gorman, Alliance for Securing Democracy, *Committee Hansard*, 21 April 2023, p. 14. The *Prague Proposals on Cyber Security of Emerging and Disruptive Technologies* were introduced at the Prague 5G Security Conference in 2021. They promote strategic thinking about security of emerging and disruptive technologies in the context of national security.

¹⁴ Ms Lindsay Gorman, Alliance for Securing Democracy, *Committee Hansard*, 21 April 2023, p. 11.

¹⁵ Ms Lindsay Gorman, Alliance for Securing Democracy, *Committee Hansard*, 21 April 2023, p. 11.

media and internet companies’ and further recommended that any company that ‘refuses to comply with such frameworks should not be able to operate in Australia’.¹⁶

- 5.23 ASIO noted that social media ‘has benefited from an era of unprecedented connectivity with limited regulation, thus creating the conditions to allow disinformation and misinformation to proliferate and indeed flourish’ and further noted that there are few laws governing online activity and the extraterritorial nature of the activity means that attribution to a foreign power ‘can be difficult to ascertain, even where such laws come into play’.¹⁷

Proportionality

- 5.24 While calling for greater regulation of social media platforms to protect Australians from foreign interference, many expert organisations also noted the need for proportionality, whereby the solutions did not stray too far into the realm of curtailing the freedoms that are the bedrock of liberal democracies.
- 5.25 The AHRC noted that ‘social media can be used for purposes that both strengthen or undermine Australia’s democracy and values’ and further advised:

Striking the right balance between regulating online activities and protecting free expression is an ongoing challenge. While there is a clear need to combat misinformation and disinformation online, there is also a risk that in doing so different perspectives and controversial opinions may be targeted. While reasonable minds may differ on exactly where the line should be drawn, if we fail to ensure robust safeguards for freedom of expression online, then the very measures taken to combat misinformation and disinformation could themselves risk undermining Australia’s democracy and values.¹⁸

- 5.26 Mr Kenny Chiu, a former Canadian MP who had been subjected to foreign interference during an election also argued against ‘blunt tools’ and called for proportionality that will ‘protect what we have treasured and worked so hard for while at the same time countering the disinformation and interference that we are facing together—not just as Australians but also with other countries such as Canada, the UK and the US’.¹⁹
- 5.27 Human Rights Watch noted that it does not support bans because it wants to see free speech and freedom of expression, ‘but we want there to be credible

¹⁶ Australian Human Rights Commission, *Submission 9*, p. 14.

¹⁷ Australian Security Intelligence Organisation, *Submission 2*, pp. 4 and 5.

¹⁸ Australian Human Rights Commission, *Submission 9*, pp. 3 and 8–9.

¹⁹ Mr Kenny Chiu, Private capacity, *Committee Hansard*, 21 April 2023, p. 18.

news sources, and for people in these communities to be aware of these alternative news sources'.²⁰

- 5.28 Meta also argued in favour of regulation being considered 'with regard to individual human rights, such as freedom of expression, freedom of speech, access to information and, of course, privacy'.²¹
- 5.29 There was extensive discussion on the issue of censorship and this discussion is captured below in the section on the new proposed powers for the Australian Communications and Media Authority (ACMA).

Proposed new powers for the Australian Communications and Media Authority

- 5.30 In June 2023, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (Department of Communications) released an exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 (Disinformation bill).
- 5.31 In its report on digital platforms' disinformation measures discussed in Chapter 3, the ACMA noted that while steps being taken under the voluntary *Australian Code of Practice on Disinformation and Misinformation* (DIGI code) were good first steps, the ACMA recommended it have 'a graduated set of new powers to combat misinformation and disinformation across the sector' which would 'increase transparency and ensure that digital platform services are held to account if voluntary industry efforts prove to be inadequate'.²²
- 5.32 In response to that report, the proposed powers in the Disinformation bill have been crafted to:
- Enable the ACMA to gather information from platforms and require digital platform providers to keep certain records about matters regarding mis and disinformation.
 - Enable the ACMA to request industry develop a code of practice covering measures to combat mis and disinformation on digital platforms, which the ACMA could register and enforce.
 - Allow the ACMA to create and enforce an industry standard (a stronger form of regulation), should a code of practice be deemed ineffective in combatting mis and disinformation on digital platforms.²³

²⁰ Ms Elaine Pearson, Asia Director, Human Rights Watch, *Committee Hansard*, 21 April 2023, p. 6.

²¹ Ms Mia Garlick, Regional Director of Policy, Meta, *Committee Hansard*, 11 July 2023, p. 2.

²² Department of Infrastructure, Transport, Regional Development, Communications and the Arts (Department of Communications), *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—Fact sheet*, June 2023, p. 3.

²³ Department of Communications, *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—Fact sheet*, p. 1.

- 5.33 Digital Industry Group Inc. (DIGI), the industry body responsible for the current DIGI code, has expressed in principle support for the proposed powers outlined in the ACMA's report.²⁴
- 5.34 The Department of Communications outlined that the intent of the Disinformation bill is to:
- ...tackle content that is reasonably likely to cause or contribute to serious harm. That, in a sense, is the intent of the bill: in a sense, for digital platforms to take steps and responsibility for the content on those platforms and, in doing so, take steps to address content that they judge could be likely to cause serious harm. So the focus is on the harm and the content rather than the intent or the source of the content, if that makes sense.²⁵
- 5.35 The Disinformation bill defines misinformation and disinformation as follows:
- Misinformation is online content that is false, misleading or deceptive, that is shared or created without an intent to deceive but can cause and contribute to serious harm.
 - Disinformation is misinformation that is intentionally disseminated with the intent to deceive or cause serious harm.
 - Serious harm is harm that affects a significant portion of the Australian population, economy or environment, or undermines the integrity of an Australian democratic process.²⁶
- 5.36 ASPI did not agree that the above definitions were clear enough, 'so it leaves subjectivity to the social media providers to decide what the litmus is for content that should be taken down'.²⁷
- 5.37 Meta described the current model of the voluntary DIGI code as 'a good way to both address the concerns of policymakers and communities about the transparency of the approach that we take to combatting misinformation and foreign interference, while also balancing the very important imperative of protecting free expression and making sure we're not overly censoring people online'. Meta further argued that the draft legislation goes further than just enforcing the DIGI code, and Meta warned that it saw 'some potential for that

²⁴ Digital Industry Group Inc, '[DIGI Welcomes The Government Providing ACMA With Oversight Powers Over Misinformation](#)', *Media release*, 20 January 2023.

²⁵ Mr Richard Windeyer, Deputy Secretary, Communications and Media Group, Department of Communications, *Committee Hansard*, 12 July 2023, p. 25.

²⁶ Department of Communications, *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—Fact sheet*, p. 1.

²⁷ Ms Emily Mosely, International Cyber Policy Centre Coordinator, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 21.

power to be abused or for it to be used in a way inadvertently chills free and legitimate political expression online’.²⁸

- 5.38 The Department of Communications disagreed with the premise that the Disinformation bill may have an unintended consequence of censorship or chilling of online discourse, however it did concede that overall effect of the draft bill would censor people who shared content that was unintentionally false, but only where that content causes serious harm.²⁹
- 5.39 Google and YouTube stated it was still working on reaching a formal position on the bill, but expressed initial support for the proposals, including giving the ACMA the powers to enforce the DIGI code. Google reminded the committee that it was one of the first signatories to the DIGI code, and wanted more companies to sign up to increase its coverage.³⁰
- 5.40 In media reports, Victorian barrister Peter Clarke described the Disinformation bill as a ‘dangerous piece of legislation’ and noted that the definition of what constitutes harm were ‘so vague as to be dangerous’. Similarly, Sydney barrister Jeffrey Phillips SC said the bill ‘poses the ability to censor and shuts down debate’ and was a ‘bad direction for us to be going in’.³¹
- 5.41 The Department of Communications is undertaking a consultation on the exposure draft, seeking submissions by 6 August 2023, which will inform any changes to the draft bill.³²

Legal remedies

- 5.42 In addition to the sector-wide approach of regulating platforms to ensure they are compliant with meeting responsibilities to reduce CIB, the committee heard that more could be done to improve the legal frameworks for reporting and charging people over instances of suspected foreign interference.

Improved reporting

- 5.43 The Australian Federal Police (AFP) stressed that reporting instances of suspected foreign interference is the first line of defence:

²⁸ Mr Josh Machin, Head of Public Policy, Australia, Meta, *Committee Hansard*, 11 July 2023, pp. 5–6.

²⁹ Mr Richard Windeyer, Department of Communications, *Committee Hansard*, 12 July 2023, p. 25.

³⁰ Ms Rachel Lord, Senior Manager, Government Affairs and Public Policy, YouTube, Google, *Committee Hansard*, 11 July 2023, p. 37.

³¹ Rhiannon Down and Sarah Ison, “Dangerous and Orwellian”: Tech giants and lawyers warn on Labor misinformation bill’, *The Australian*, 11 July 2023.

³² Department of Communications, *New ACMA powers to combat misinformation and disinformation*, www.infrastructure.gov.au/have-your-say/new-acma-powers-combat-misinformation-and-disinformation (accessed 17 July 2023).

Senator, my personal view is that the best strategy to defend against foreign interference is through high community and agency awareness and also knowledge of how to report it. If it's reported, we're able to understand it. And once we're able to understand it, we can work to disrupt and look at vulnerabilities that need to be corrected not only on individual case basis, but at more system level.³³

- 5.44 The AFP advised that foreign interference allegations 'come to us through a number of means ... through Crime Stoppers, through direct reports to the AFP, referred from other departments, as well as through the National Security Hotline, as well as other government departments'.³⁴ ASIO likewise submitted that it has a number of channels for the reporting of concerns about being contacted for the purpose of foreign interference for clearance holders, members of the public, government organisations, and private sector companies.³⁵
- 5.45 Home Affairs likewise stressed the importance of people reporting instances of foreign interference through the National Security Hotline and noted that 'there are certainly times when there is an increase in certain communities reporting suspected foreign interference or interference, and we work very closely with those communities and will step up engagement with those communities to respond to that when we see those occurring'.³⁶
- 5.46 Mrs Kateryna Argyrou of the Australian Federation of Ukrainian Organisations told the committee that her organisation made sure to report all instances of harassment and interference:

Every time we've had a community member who has been harassed online or threatened—and we've had many community members who've received death threats through Telegram channels, through Facebook Messenger and through other social media—we've reported that [to the] the police.³⁷

- 5.47 Mr Peter Murphy of Australian Supporters of Democracy in Iran noted the challenges faced by people in reporting foreign interference but that once reported, it appeared to be taken seriously:

It was a bit of a merry-go-round. We'd ring the Federal Police, and they'd say go to the New South Wales police. We'd ring the New South Wales police, and they'd say go to the Federal Police, so eventually I had to go in person to the Federal Police during the pandemic because nobody would really talk on the phone. But I think it was a reasonable exchange. I was

³³ Mr Stephen Nutt, Commander, Special Investigations, Counter Terrorism and Special Investigations Command, Australian Federal Police, *Committee Hansard*, 12 July 2023, p. 22.

³⁴ Mr Stephen Nutt, Australian Federal Police, *Committee Hansard*, 12 July 2023, p. 23.

³⁵ Australian Security Intelligence Organisation, *Submission 2*, p. 6.

³⁶ Ms Sally Pfeiffer, Acting First Assistant Secretary, Counter Foreign Interference, Department of Home Affairs, *Committee Hansard*, 12 July 2023, p. 8.

³⁷ Mrs Kateryna Argyrou, Co-Chair, Australian Federation of Ukrainian Organisations, *Committee Hansard*, 21 April 2023, p. 28.

interrogated or questioned and was able to convey all the information I wanted to give, and it was taken seriously ... I'm more confident that our agencies are getting a clearer view of what is going on and are more willing to take action to protect people here than they might have been before.³⁸

5.48 However, Human Rights Watch raised concerns that members of diaspora communities in Australia who may be subjected to threats and intimidation 'don't know what to do about those threats or who to report them to' and recommended an information campaign to advise diaspora communities in Australia, including in other languages, not just English.³⁹

5.49 The AFP noted that due to the sensitivities of the reported issues, people reporting via the National Security Hotline were generally not kept informed of progress on the matter they reported, and sometimes were not even acknowledged that a report had been made. However, the AFP did stress the continued importance of making such reports, particularly because reports are then sent to 'multiple agencies and agencies that need to know'.

5.50 The AFP went on to advise that:

In terms of our response, we look at matters on a harm basis. So a high-harm report is something that is prioritised now. High harm in terms of community interference, or foreign interference in community, or transnational repression—it depends on which stream you're listening to—is really where there are actual threats or demands with menace that involve the potential for serious physical harm being directed at a person or a community. Those are the priority areas that we look at.⁴⁰

5.51 The AFP further advised that 'The biggest challenge, as I pointed out earlier, is that foreign principal element. I know that there is a quantum of reporting where people are feeling intimidated or feeling that they're subject to foreign interference. In our case, if we are unable to establish a foreign actor involvement, that does limit our ability to respond under the foreign interference legislation'.⁴¹

Charges and prosecution

5.52 Despite the prevalence of social media-based foreign interference, harassment and threats being experienced by diaspora communities in Australia—many of whom are Australian citizens—the AFP advised the committee there had been no instances where a person was charged under the *National Security Legislation*

³⁸ Mr Peter Murphy, Co-Secretary, Australian Supporters of Democracy in Iran, *Committee Hansard*, 21 April 2023, p. 21.

³⁹ Ms Elaine Pearson, Human Rights Watch, *Committee Hansard*, 21 April 2023, pp. 4–5.

⁴⁰ Mr Stephen Nutt, Australian Federal Police, *Committee Hansard*, 12 July 2023, p. 18.

⁴¹ Mr Stephen Nutt, Australian Federal Police, *Committee Hansard*, 12 July 2023, p. 18.

Amendment (Espionage and Foreign Interference) Act 2018 (Espionage Act) with foreign interference via a social media platform.⁴²

- 5.53 The AFP advised the committee of the range of elements that must exist in order for foreign interference to meet the threshold for offences under the Espionage Act:

... our primary consideration is the involvement of a foreign actor and whether an individual is working in collaboration with a foreign actor or as a proxy. That's a key requirement. And then obviously we have to look at the other elements of the offence, whether it goes to government processes, political processes, political rights or democratic rights being exercised, and whether an intelligence objective of the foreign principal is what the activity is related to or it's adverse against the national security of Australia. We then consider whether the conduct involved an element of covert and deception or whether there was a threat of serious harm or the demand with menace. That's the collective of what needs to be proven.⁴³

- 5.54 The AFP did note that where an action might not meet the threshold of the Espionage Act—which requires either a foreign principal or a proxy of a foreign principal to be undertaking the action—the action may still be a crime under other laws:

There also may be other criminal investigations, because conducting a threat or harassment or menace online is a separate offence, not under the foreign interference legislation...And of course if the posting is potentially hate crime related, this is not a Commonwealth jurisdiction; it's something that will fall to state and territory police.⁴⁴

- 5.55 The AFP stressed that 'no report is lost' and outlined that where there are individuals who are criminally targeting the community, the AFP does prioritise those reports. Where it does not fall within its jurisdiction, they refer to state and territory police and advised the committee that 'we don't just not respond'.⁴⁵

- 5.56 ASIO also noted a range of activities it can undertake where charges cannot be laid:

There are other things we do in the course of our engagement. We can engage with victims as well as perpetrators of foreign interference or people that we believe are likely to be involved in perpetrating foreign interference. That can have an effect of adding resilience, rendering the environment less permissive, if you like. I wouldn't go into the nature of those engagements. They're confidential by their nature. The point I'd leave you with is that the taskforce has a range of options at its disposal to seek to disrupt and reduce

⁴² Mr Stephen Nutt, Australian Federal Police, *Committee Hansard*, 12 July 2023, p. 16.

⁴³ Mr Stephen Nutt, Australian Federal Police, *Committee Hansard*, 12 July 2023, p. 17.

⁴⁴ Mr Stephen Nutt, Australian Federal Police, *Committee Hansard*, 12 July 2023, p. 23.

⁴⁵ Mr Stephen Nutt, Australian Federal Police, *Committee Hansard*, 12 July 2023, p. 24.

the harm from foreign interference, including what we call community interference or transnational repression.⁴⁶

5.57 The Law Council of Australia noted that widespread use of the foreign interference offences under the Espionage Act and the *Criminal Code Act 1995* (Criminal Code) was unlikely 'given the challenges that exist in relation to successfully investigating and prosecuting persons who commit this offence when the "conduct" occurs outside Australia'. Nevertheless, the Law Council of Australia suggested that these measures could still prove useful in conjunction with other approaches.⁴⁷

5.58 This was supported by evidence from witnesses such as Mrs Kateryna Argyrou from the Australian Federation of Ukrainian Organisations, who told the committee:

Last time I checked, we'd had over 40 official complaints registered with police, with registered numbers. We continue to add to that list. The Australian law enforcement agencies have been very open and willing to listen, but I think there is an issue here between where they can use the full force of the law and where they can just sympathise and say, 'We hear you, but there is really nothing we can do' ... So this is where we would hope that you [this inquiry] can hear our concerns on that point of view, and something can be discussed or done on that front.⁴⁸

5.59 A joint submission from technical specialist University centres suggested that changes to relevant laws would be necessary to enable the use of technical methods and tools relating to the monitoring or investigation of foreign interference through social media and their results in judicial proceedings, writing:

Litigation is a potential, but currently inadequate, antidote to disinformation. Litigation removes individuals from their informational bubbles or echo chambers, assign neutral judges or regulators - instead of simply the marketplace of ideas - to render a judgment on the truth or falsity of certain beliefs and compel action by responsible parties. However, litigation has not yet delivered on its potential. For example, criminal prosecution of offenses of foreign interference through social media, while theoretically possible, is often dismissed as practically infeasible given the jurisdictional and evidentiary challenges.⁴⁹

⁴⁶ Mr Mike Noyes, Deputy Director-General, Intelligence Service Delivery, Australian Security Intelligence Organisation, *Committee Hansard*, 12 July 2023, p. 10.

⁴⁷ Law Council of Australia, *Submission 27*, pp. 2–3.

⁴⁸ Mrs Kateryna Argyrou, Australian Federation of Ukrainian Organisations, *Committee Hansard*, 21 April 2023, p. 28.

⁴⁹ Joint University Submission, *Submission 19*, pp. 6–7.

Countermeasures

5.60 The committee heard that in addition to the significant gaps in identifying and reporting foreign interference, there are gaps in Australian Government countermeasures once foreign interference is detected.

5.61 Overall, the committee heard the government should operate with greater transparency, including by being less reticent to 'call out' instances of foreign interference and providing advice on security concerns, and that countermeasure operations should be conducted under a more rigorous framework, such as those being used in the European Union (EU) and United States (US).

5.62 Dr Andrew Dowes, Director of RAND Australia advised that governments should be taking an analytical approach to developing countermeasures:

It may be instructive to consider how an actor, whether it be foreign or domestic, might go about undertaking a disinformation campaign in order to understand how then that influence could be countered at each step of the disinformation process. In my view these problems of disinformation and information are not able to be defeated by a single action, but require a series of interventions, ranging from addressing the motivation of actors to addressing structural issues in social media networks, to various ways of reducing the likelihood of the audience believing or amplifying force content. In my view such interventions should be priorities for our government, as otherwise the risks and potential consequences of interference through social media will just continue to get worse.⁵⁰

Transparent government communication

5.63 The AHRC argued that any taskforce addressing foreign interference should, where possible, report more publicly than is currently done 'to bring greater transparency to the ways in which misinformation and disinformation are being addressed both to enhance the public understanding of the risks to Australia, and ensure that other rights and freedoms are not disproportionately impacted'.⁵¹

5.64 ASPI noted the success experienced by other governments being more willing to call-out interference operations:

So the question [is]...how do we shift the adversary's thinking about conducting these operations? For state actors, it might be about imposing diplomatic costs or pointing out that they are doing that and imposing a solution of just calling them out and sort of naming and shaming them. I think, at the international level, through multilateral agreements, there is a lot of scope for governments to make those public attributions. That does

⁵⁰ Dr Andrew Dowse, Director, RAND Australia, *Committee Hansard*, 20 April 2023, p. 27.

⁵¹ Australian Human Rights Commission, *Submission 9*, p. 8.

two things: it does deterrence but it does educate the public as well...Calling them out does really impose costs, and I think it is an easy win, really.⁵²

5.65 Ms Elaine Pearson, Asia Director, Human Rights Watch advised that:

...there is also a really important role that the Australian government can play in ensuring that the acts of intimidation, harassment and censorship that occur on apps like WeChat are publicised. Chinese-language communities in Australia need to be aware of that, and it shouldn't just be up to civil society organisations or think tanks, really, to be disclosing these incidents.⁵³

5.66 Dr William Stolz also argued that in addition to reacting to single instances of foreign interference, 'we need to be engaging in our own information operations to push our own positive narratives—again accepting that effectiveness is going to be ambiguous, but it is perhaps better to be proactive in pushing our own narratives into what is a maelstrom information environment and hope that we achieve a positive impact'.⁵⁴

5.67 Professor Rory Cormac agreed and noted that this type of response should not be restricted to 'setpiece events like elections or regime change' but should 'counter that daily drip of disinformation, interference and subversion on an intangible level, which just seeks to sow confusion and discord, exploit pre-existing schisms in society, and gradually chip away at trust in institutions like democracy'. Professor Cormac further noted the recent countermeasures taken by the UK's National Cyber Force as showing 'nuance, maturity and evolution'.⁵⁵

Advising on security concerns

5.68 As discussed in earlier chapters, TikTok was banned from being installed on Australian Government-issued devices. A gap was discussed in relation to organisations providing contracted services to government.

5.69 The Attorney-General's Department advised that the Protective Security Policy Framework (PSPF) 'requires non-corporate Commonwealth entities to be accountable for security risks arising from any contractual arrangements they have and to then place security requirements on those they contract'. This was explained to mean that any entity with obligations under the PSPF must ensure

⁵² Mr Albert Zhang, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 25.

⁵³ Ms Elaine Pearson, Human Rights Watch, *Committee Hansard*, 21 April 2023, p. 3.

⁵⁴ Dr William Stoltz, Private capacity, *Committee Hansard*, 20 April 2023, p. 38.

⁵⁵ Professor Rory Cormac, Director, Centre for the Study of Subversion, Unconventional Interventions and Terrorism, University of Nottingham, *Committee Hansard*, 20 April 2023, p. 39.

that external contractors who work with sensitive government information must also adhere to the same risk approach to applications such as TikTok.⁵⁶

- 5.70 However, the Attorney-General's Department did concede that level of granular detail was not expected to be reported by departments in their annual reporting on their compliance with the PSPF, so whether or not departments had turned their minds to applying the ban to government contractors would not be known.⁵⁷

Regulated frameworks

- 5.71 Chapter 3 on international issues provided an extensive outline of the foreign interference approaches being used in the EU and US, such as the Disinformation Analysis and Risk Management (DISARM) open-source framework for analysis of interference instances and its 'kill-chain' approach to countermeasures.

- 5.72 RAND Australia submitted that because a disinformation campaign involves a sequence of steps 'for false information to be created, disseminated, observed and amplified', that creates opportunities for countermeasures at each step, only one of which needs to be successful to knock out the whole chain.

Countering efforts at each of these steps may help mitigate the impact of disinformation, including the use of information by actors that represents foreign interference. A strong countering strategy should combine such efforts within a survival chain, rather than expecting a singular solution to defeat disinformation.⁵⁸

- 5.73 Dr Andrew Dowse, Director of RAND Australia, expanded on this directly to the committee, citing the kill-chain philosophy being increasingly used in the EU as a tactic to address foreign interference:

The steps to enabling a disinformation campaign go from the considering of the strategy and the message to setting up the means by which the message can be provided and transmitting the message. So there are steps. The countering of that is not necessarily sequential but can be concurrent. Some of the countering of those steps could be proactive. Some could be responsive. None of them are mutually exclusive, which is why I suggested you need lots of lines of effort.

It's like a defence in depth, where some will get through the first step and some will get through the third but, through all those lines of effort, you should defeat a majority of those activities...this kill chain/survival chain concept has been applied in cybersecurity, very effectively, and I think it

⁵⁶ Ms Sarah Chidgey, Deputy Secretary, National Security and Criminal Justice, Attorney-General's Department, *Committee Hansard*, 12 July 2023, p. 20.

⁵⁷ Ms Sarah Chidgey, Attorney-General's Department, *Committee Hansard*, 12 July 2023, pp. 20–21.

⁵⁸ RAND Australia, *Submission 11*, p. 3.

lends itself very well to attempting to defeat disinformation campaigns as well.⁵⁹

International cooperation

5.74 Ms Lindsay Gorman of the Alliance for Securing Democracy advised that Australia:

... join with democratic allies and partners to develop a comprehensive framework for addressing the threats posed by authoritarian internet apps and critical information infrastructure. Given Australia's strong work on foreign interference, it is naturally poised to take a leading role in these efforts.⁶⁰

5.75 Meta similarly called for a global collaborative approach, noting that 'combatting foreign interference requires multisectoral, whole-of-society approaches towards building a strong security ecosystem not only within Australia but across the region and globally'.⁶¹

Cross-sector collaboration

5.76 The committee heard that greater collaboration between government, tech firms and civil society experts would not only improve coordination of overall countermeasures, but would help each sector in the specific areas they are responsible for. The areas of threat intelligence and technical research were particularly called out.

5.77 Meta argued for 'greater information sharing of IO threat signals among tech companies and between platforms, civil society and government, while protecting the privacy of innocent users who may be swept up in these campaigns'.⁶²

5.78 Both ASIO and Home Affairs noted that they do not share intelligence on specific instances of suspected foreign interference. Home Affairs advised:

We don't undertake referrals about specific pieces of information in relation to foreign interference. Our engagement with social media platforms is to the level of the broader understanding of misinformation and disinformation and how it could be used and the processes that the social media platforms might themselves look at with their terms of use and the referrals they receive regarding concerns.⁶³

⁵⁹ Dr Andrew Dowse, RAND Australia, *Committee Hansard*, 20 April 2023, p. 29.

⁶⁰ Ms Lindsay Gorman, Alliance for Securing Democracy, *Committee Hansard*, 21 April 2023, p. 9.

⁶¹ Ms Mia Garlick, Meta, *Committee Hansard*, 11 July 2023, p. 2.

⁶² Meta, *Submission 32*, p. 17.

⁶³ Ms Sally Pfeiffer, Department of Home Affairs, *Committee Hansard*, 12 July 2023, p. 12.

5.79 ASIO advised that:

One of the challenges we'd have there is that even in those circumstances where we can identify it, providing that intelligence to individuals or companies that don't employ individuals with clearances is a real challenge for us.⁶⁴

5.80 Both Home Affairs and ASIO noted there was no policy reason they were aware of that would preclude social media employees from seeking security clearances, and Home Affairs advised it would then allow them to share some information.

5.81 In regards to technical research, the issue of funding arose. Meta recommended there should be more support for private and public 'innovation and collaboration on technical detection of adversarial threats such as manipulated media, including deepfakes'.⁶⁵

5.82 Dr Dowse of RAND Australia noted the limited funding avenues to undertake research on social media data. He advised that RAND Australia had to seek US funding to undertake research on Australian issues, and stated 'I would dearly like to see the Australian government perhaps providing more sources of funding so we can do this research'.⁶⁶

5.83 The following chapters, on platforms and civil society responsibilities, discusses the issue of technical research in greater detail.

⁶⁴ Mr Mike Noyes, Australian Security Intelligence Organisation, *Committee Hansard*, 12 July 2023, p. 12.

⁶⁵ Meta, *Submission 32*, p. 17.

⁶⁶ Dr Andrew Dowse, RAND Australia, *Committee Hansard*, 20 April 2023, p. 28.

Chapter 6

Platforms

Current practice and identified gaps

- 6.1 The introductory chapters to this report outlined the important and central role that social media plays in the lives of many Australians, and that depending on how it is used, social media can either strengthen or undermine democracy. Further, it was noted that because of its depth and reach into nearly every single person's life, social media is being increasingly used as a vector for foreign interference.
- 6.2 While some technology firms are taking some steps towards addressing the issue of foreign interference on their social media platforms, this chapter outlines the overwhelming evidence that nowhere near enough is being done.
- 6.3 An additional specific area of risk is social media platforms which originate from authoritarian states. These issues are discussed separately, in acknowledgement of the particular risks posed.

Platform responsibilities

- 6.4 Social media companies have responsibilities for content published on their platforms. With regard to foreign interference, the *Australian Code of Practice on Misinformation and Disinformation* (DIGI Code), while voluntary, does require platforms to 'address concerns regarding disinformation and credibility signalling for news content'.¹
- 6.5 The Australian Communications and Media Authority (ACMA) noted that the DIGI Code only has eight signatories.² The ACMA stated there are a number of platforms operating in Australia which chose not to become part of the code, and the ACMA is aware of the 'extent to which there might be misinformation and disinformation which has the risk of contributing to serious harm'. The ACMA stated it had engaged with a number of those platforms over the years and encouraged them to join the code. The ACMA further noted that Digital Industry Group Inc. (DIGI) had updated the code's reporting

¹ Digital Industry Group Inc (DIGI), [Australian Code of Practice on Misinformation and Disinformation](#), Updated 22 December 2022, p. 2.

² Signatories include: Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitter.

requirements to reduce the reporting burden for, digital platforms, so it hoped that might result in some platforms electing to sign up to the DIGI Code.³

- 6.6 The ACMA noted that it would be looking at information reporting requirements under a similar code operating in Europe, to compare and contrast with what platforms are reporting in Australia.⁴

Platform actions to address interference

- 6.7 Platforms provided details to the inquiry on actions they take to address foreign interference. Platforms noted their actions are targeted to address any instances of coordinated inauthentic behaviour (CIB), regardless of whether it is for the purpose of foreign interference or is undertaken by non-state actors (often financially motivated).

Meta actions

- 6.8 In its submission, Meta (which owns Facebook, Instagram, WhatsApp and the newly launched Threads) outlined for the committee the three main strategies it uses to combat foreign interference via its platforms, which include:
- automated defences that leverage machine learning to detect and block bad actors: such as systems that find and block millions of fake accounts every day, most within minutes of creation;
 - threat intelligence analysts who hunt for and disrupt CIB not caught by the automated defences; and
 - collaboration by sharing information with counterparts in industry and with government, civil society and the media.⁵
- 6.9 The Department of Home Affairs (Home Affairs) noted the work undertaken by Meta, submitting that between 2017 and 2022 'Meta disabled and publicly reported on over 200 covert influence operations that violated its policies' and that these operations 'originated from over 60 countries and targeted both foreign nations and their own domestic public debate'.⁶

Twitter actions

- 6.10 Mr Nick Pickles, Head of Global Government Affairs, Twitter, told the committee that Twitter has an approach of early intervention when it suspects foreign interference or CIB, and due to the difficulties in definitively attributing content Twitter doesn't necessarily wait for this before taking action:

³ Ms Cathy Rainsford, General Manager, Content and Consumer Division, Australian Communications and Media Authority, *Committee Hansard*, 12 July 2023, pp. 28–29.

⁴ Ms Nerida O'Loughlin, Chair, Australian Communications and Media Authority, *Committee Hansard*, 12 July 2023, p. 29.

⁵ Ms Mia Garlick, Regional Director of Policy, Meta, *Committee Hansard*, 11 July 2023, p. 2.

⁶ Department of Home Affairs, *Submission 1*, p. 3.

Often we're looking at behaviour signals. They may be linked to accounts, networks or origin. Obviously many of these actors are trying to hide and obfuscate where they are, so it's not as simple as saying, 'Show me all the Twitter accounts from one country.' We look at content.

- 6.11 Mr Pickles then cited initiatives such as Community Notes, verification and Twitter Blue as additional programs designed to capture CIB. Community Notes was explained as allowing people on Twitter to add context to other people's tweets:

Those tweets can be added to any account, including advertisers, political leaders and prominent influencers. By looking at the people who are adding that data, we're already seeing a significant impact, with an up to 35 per cent reduction in the sharing of those accounts based on context added by other users.⁷

LinkedIn

- 6.12 LinkedIn presents a different risk for foreign interference than other social media platforms, as it is a professional networking site. In February 2023, the Australian Security Intelligence Organisation (ASIO) head Mr Mike Burgess noted that ASIO identified nearly 16 000 Australians publicly declaring on professional networking sites they have a security clearance, and 1 000 more revealing they worked in the intelligence community. Mr Burgess said 'these people may as well add "high-value target"' to their profiles.⁸
- 6.13 In recent years, LinkedIn has become heavily abused by threat actors seeking to distribute malware, perform cyberespionage, steal credentials, or conduct financial fraud. In 2022, LinkedIn was used by Lazarus North Korean hacking group for cybercriminal and espionage operations, contacting victims via targeted private messages on the platform.⁹
- 6.14 LinkedIn noted that the largest threat is posed by fake accounts and reported that in 2022 it 'blocked more than 80 million fake accounts worldwide, of which about 400 000 were attributed to Australia'.¹⁰

Google and YouTube

- 6.15 Google and YouTube provided information to the committee on steps it takes to address foreign interference on its platforms, via the Threat Analysis Group (TAG), a 'global team of analysts and security experts that analyses and counters

⁷ Mr Nick Pickles, Head, Global Government Affairs, Twitter, *Committee Hansard*, 11 July 2023, pp. 42 and 43.

⁸ Casey Tonkin, '[Don't put your security clearance on LinkedIn](#)', *InformationAge*, 23 February 2023.

⁹ Veronica Chierzi and Mayra Rosario Fuentes, '[A Growing Goldmine: Your LinkedIn Data Abused For Cybercrime](#)', *TrendMicro Business*, 28 March 2023.

¹⁰ Mr Joshua Reiten, Senior Director, Legal—Digital Safety, LinkedIn, *Committee Hansard*, 11 July 2023, p. 16.

serious threats to Google and our users, including threats from government backed attackers, serious cybercriminals and information operations'.¹¹

6.16 In relation to countermeasures taken by YouTube, the committee was told:

We particularly focus on disrupting coordinated influence operations on YouTube. For example, in the first quarter in 2023 we terminated more than 900 YouTube channels linked to Russia and more than 18,000 linked to China, as part of our investigations into coordinated influence operations. These actions are in addition to YouTube's ongoing enforcement of community guidelines, which resulted in the removal of more than 5.6 million videos globally in the fourth quarter of 2022.¹²

6.17 However, YouTube did acknowledge that even in the recent past (2021) it had not always responded to remove harmful content as fast as it should have.¹³

WeChat

6.18 WeChat made a submission to the inquiry, as it did to the similar inquiry of the 46th Parliament, however that submission contained no specific information on how it addresses disinformation, surveillance, censorship, disinformation or CIB on its platform. Notably, WeChat repeatedly declined multiple invitations to participate in a public hearing to answer direct questions from the committee, ignoring that the invitation allowed them to participate via videoconference from any location in the world as other witnesses utilised.¹⁴

6.19 On 4 July 2023, as Chair of the Select Committee, Senator James Paterson sent an open letter to WeChat urging them to reconsider their refusal to appear in a public hearing. On 10 July 2023, WeChat responded to Senator Paterson to reiterate their stated intention of 'working collaboratively with Australian regulators and authorities' and said that it remained 'committed to providing responsive information to the committee in writing' but continued to refuse to front up in an open forum.¹⁵

6.20 In doing so, WeChat has demonstrated contempt for the Australian Parliament and has shown the Australian public that WeChat, and their parent company Tencent, is not genuinely committed to being held accountable for the serious allegations of censorship, surveillance and foreign interference at the hands of

¹¹ Mr Shane Huntley, Senior Director and Global Lead, Google Threat Analysis Group, Google, *Committee Hansard*, 11 July 2023, p. 35.

¹² Mr Shane Huntley, Google, *Committee Hansard*, 11 July 2023, p. 35.

¹³ Ms Rachel Lord, Senior Manager, Government Affairs and Public Policy, YouTube, Google, *Committee Hansard*, 11 July 2023, p. 36.

¹⁴ WeChat, *Submission 15*, pp. 3–4.

¹⁵ Senator James Paterson, 11 July 2023, available at <https://twitter.com/SenPaterson/status/1678557229883207681> (accessed 26 July 2023).

the Chinese Communist Party (CCP) which is rife on its platform and is a real concern to WeChat users in Australia.

- 6.21 Senator Paterson, on behalf of the committee, submitted 53 detailed questions to WeChat asking for an explanation on its links to the CCP, whether it censors content critical of the Chinese Government and promotes CCP propaganda, and whether the application is used to surveil and target Australian users critical of the regime, including its human rights record.
- 6.22 WeChat was initially required to respond by 21 July 2023, however WeChat requested via the secretariat an extension of time and was given until 26 July 2023 to provide answers to these 53 questions.
- 6.23 WeChat submitted its response to these 53 questions on 26 July 2023, however unfortunately WeChat failed to meet the transparency test by not providing direct answers to the questions that were asked of them.
- 6.24 WeChat flatly denies censorship, surveillance and control is being exercised on the platform even though this has been repeatedly and convincingly demonstrated by independent researchers and experts, including those who testified before the committee.
- 6.25 In relation to censorship on the platform, Dr Seth Kaplan testified that WeChat is:

... doing the censoring for the party, and there are what you might call united front and other agents whose content, basically, is being promoted ... There is extensive censorship, there is extensive demoting, people are being banned and people are being suspended ... I wouldn't say that the CCP is directly doing it. I think Tencent is under instructions on how it must manage the platform.¹⁶

- 6.26 In relation to surveillance and control on WeChat, Dr Kaplan added:

... you have to understand that this surveillance and control of the [Chinese] diaspora operates on two levels. One is WeChat, and then there are individuals. They could be United Front; they could be other actors...or they may be just rabid nationalists ... The non-WeChat avenues for monitoring, constraining and controlling this vulnerable population would be much less effective if there were no WeChat.¹⁷

- 6.27 On WeChat's links to the CCP, CyberCX submitted that the 'risk that the dominant position of social media platforms is abused by malign actors is heightened for platforms, such as TikTok and WeChat, which are linked to authoritarian governments'. Internet 2.0 argued in their submission that 'we consider that WeChat is under structural pressure to support the CCP's rule of

¹⁶ Dr Seth Kaplan, Private capacity, *Committee Hansard*, 20 April 2023, p. 13.

¹⁷ Dr Seth Kaplan, *Committee Hansard*, 20 April 2023, p. 16.

law. We believe this structural market pressure may come at a disadvantage to all other governments' rule of law'.¹⁸

- 6.28 The Australian Strategic Policy Institute's (ASPI) 2020 report into TikTok and WeChat found that WeChat has 'become the long arm of the Chinese regime, extending the PRC's [People's Republic of China's] techno-authoritarian reach into the lives of its citizens and non-citizens in the diaspora. WeChat users outside of China are increasingly finding themselves trapped in a mobile extension of the Great Firewall of China through which they're subjected to surveillance, censorship and propaganda'.¹⁹
- 6.29 WeChat's dismissive non-answers are a disingenuous effort to assist the committee by engaging in blatant spin and corporate talking points, and is further evidence for the contempt they have for the Australian Parliament.

TikTok

- 6.30 TikTok provided descriptions of actions it takes against CIB on its platform. TikTok's *Community Guidelines* 'prohibit content that could mislead our community about civic processes or matters such as public health and safety'. TikTok submitted that its community guidelines which prohibit misleading information are enforced through safety professionals and moderators, technology-based flagging and via a fact checking partnership with Australian Associated Press.²⁰
- 6.31 TikTok reported that between July and September 2022, it blocked 41 459 159 spam accounts, removed 94 733 447 videos posted by spam accounts and removed 759 044 040 fake followers. TikTok submitted that five networks of operations involved in spam account activity, fake engagement and covert influence operations on-platform were removed in the same period.²¹ However, the committee notes this appears to be the global number of removed networks, which may be considered very low when compared against reports of the prevalence of disinformation influence operations.

Ongoing concerns

- 6.32 The rest of this chapter outlines concerns raised around the success of current actions in addressing foreign interference and CIB, as well as the complete absence of action in some cases.

¹⁸ Internet 2.0, *Submission 17 Attachment 1*, pp. 4–5.

¹⁹ Fergus Ryan, Audrey Fritz, Daria Impiombato, '[TikTok and WeChat: Curating and controlling global information flows](#)', *Australian Strategic Policy Institute*, 8 September 2020.

²⁰ TikTok, *Submission 30*, pp. 4–5.

²¹ TikTok, *Submission 30*, p. 9.

Content moderation

- 6.33 The committee heard that content moderation is a concern to many stakeholders, who were thought that either platforms were not removing malignant content fast enough, or that platforms were engaging in censorship by removing content that should remain, either because of inappropriate requests from governments or due to problems with fact-checking processes.
- 6.34 The Australian Human Rights Commission (AHRC) noted that platforms use a mix of automated technology and human moderators to address disinformation, and it did not think that current efforts were adequate under the growing volumes of disinformation.²²
- 6.35 Home Affairs noted a study which found weaknesses in TikTok and Meta moderation of advertisements as part of a controlled experiment:
- TikTok failed to catch 90 per cent of ads featuring false and misleading messages about elections in the United States, while Meta was only '... partially effective in detecting and removing the problematic election ads' as part of the experiment. Similar studies conducted globally, indicate social media platform content moderation success can vary from one country to another.²³
- 6.36 ASIO submitted that it would support measures requiring platforms and service providers to dedicate specific resources to the identification and moderation of disinformation content, published on their services 'commensurate with the volume of content and reach of their services'.²⁴

Reporting content for removal

- 6.37 The removal of content which breaches platform standards has two aspects. The first is whether or not platforms are responsive to *legitimate* reports from individuals, agencies or experts on foreign interference content, and the second aspect, discussed later in this section, is how platforms respond when they receive *inappropriate* requests for content removal.
- 6.38 The committee heard from community members and expert organisations that reporting instances of foreign interference directly to platforms does not result in swift cooperation to take down content. Mrs Kateryna Argyrou, Co-Chair of the Australian Federation of Ukrainian Organisations told the committee that:

On Facebook, where we can report certain posts, videos and content, we need to have hundreds, if not thousands, of our community members reporting it. Sometimes it gets taken down; in most cases it doesn't ... we

²² Australian Human Rights Commission, *Submission 9*, p. 7.

²³ Department of Home Affairs, *Submission 1*, p. 3.

²⁴ Australian Security Intelligence Organisation, *Submission 2*, p. 6.

can report on YouTube taking action, but Facebook, which is a huge platform, to a large extent does absolutely nothing.²⁵

6.39 Conversely, Meta advised the committee that it takes an approach to 'make ourselves accessible and available to individuals and experts to come to us when they might be experiencing [harassment] is in addition to the broader systems that we have in place to detect this type of behaviour proactively and remove it.'²⁶

6.40 Ms Vicky Xu, a journalist and policy analyst, noted that current processes to remove content take far too long, particularly when the content is directed at intimidating or attacking an individual:

It took a couple of months for anything to actually happen and for YouTube to take action, and, by that time, hundreds of thousands of people had watched the content. I think there are things we can do to establish a kind of mechanism to—I can't speak more frankly than this—kill that content early and faster because that is very damaging. The same goes for platforms like Facebook and Twitter.²⁷

6.41 Ms Xu noted the balancing act between taking action to protect individuals, versus protecting against undue censorship:

How do we treat this? If the Chinese state makes a whole package of information in order to conduct character assassination against journalists who live in democracies, what is the difference between that and, for example, hate speech or violent content? I don't think that these two categories of harmful information are, by nature, very different. Currently, as I understand it, we don't have the mechanism or a way to get there fast and get rid of this content. I'm very aware that, by speaking like this, I'm encouraging censorship of a kind, but I guess this is a question I'm going to throw back to you: do we need more censorship around these things, or do people like me just drown in misinformation?²⁸

6.42 Twitter submitted that foreign interference should be approached 'as a broad geopolitical challenge, not one of content moderation', and argued that removal of content alone will not address this challenge.²⁹

6.43 Extra-territorial censorship through informal channels as foreign interference The committee heard that the system of reporting misinformation and disinformation for removal can itself be used as a tool of foreign interference or censorship and further, that some of those requests are made informally through

²⁵ Mrs Kateryna Argyrou, Co-Chair, Australian Federation of Ukrainian Organisations, *Committee Hansard*, 21 April 2023, p. 30.

²⁶ Mr Josh Machin, Head of Public Policy, Australia, Meta, *Committee Hansard*, 11 July 2023, p. 4.

²⁷ Ms Vicky Xu, Senior Fellow, Australian Strategic Policy Institute, *Committee Hansard*, 21 April 2023, p. 36.

²⁸ Badiucac, Private capacity, *Committee Hansard*, 21 April 2023, p. 36.

²⁹ Twitter, *Submission 20: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 2.

back channels by foreign governments and are not appropriately disclosed by social media platforms. This is of particular concern when requests are being made after pressure by authoritarian states, and the broader risks posed by those governments are discussed in detail later in this chapter.

- 6.44 As ASIO pointed out to the committee, there are a range of activities which, when conducted openly, would not constitute foreign interference under Australian legislation, but 'could become foreign interference if they involve the hidden hand of a foreign state'.³⁰
- 6.45 The committee heard that extra-territorial censorship, such as blacklisting, visibility limiting or manipulation of visibility undertaken by social media, on request or under pressure from foreign governments, is an activity which can 'have a direct impact on the human rights of Australians or those living in Australia, as well as undermining Australia's democracy'.³¹ This is particularly the case when requests or demands by foreign governments for social media companies to remove or reduce visibility of content, or de-boost political figures are not disclosed to the public, and where the action taken by social media companies to censor or limit content impacts on the visibility of Australian users and free political discourse in Australia.
- 6.46 As the AHRC submitted to the committee: 'social media platforms, which function as a digital "town square" for free speech and self-expression, are increasingly affected by censorship. In particular, the expansion of the internet and social media has seen increased examples of extra-territorial censorship, where governments seek to suppress speech outside of their national borders'.³² "Badiucao, a notable artist who criticises the CCP, informed the committee that in some cases, the content reporting mechanisms were used by authoritarian states to censor dissidents:
- For example, on Twitter, they would report certain accounts without any basis. But that kind of campaign was forcing the algorithm from Twitter to respond to these reports and suspend the account targeted. This methodology has been very useful and commonly used by the Chinese government to silence critical voices outside of China.³³
- 6.47 Human Rights Watch also pointed to whistleblower Peiter Zatko, Twitter's former chief security officer who claimed that the security shortcomings of Twitter constituted '[n]egligence and even complicity with respect to efforts by foreign governments to infiltrate, control, exploit, surveil and/or censor the

³⁰ Australian Security Intelligence Organisation, *Submission 2*, p. 4.

³¹ Australian Human Rights Commission, *Submission 9*, p. 15.

³² Australian Human Rights Commission, *Submission 9*, p. 15.

³³ Ms Vicky Xu, Australian Strategic Policy Institute, *Committee Hansard*, 21 April 2023, p. 36.

company's platform, staff, and operations'.³⁴ Human Rights Watch further noted:

Before Musk's purchase of the platform, Twitter had quickly reacted to requests to protect the accounts of Chinese human rights defenders. After Musk's acquisition, the gutting of the infrastructure and staff that deal with these issues threatens to change that equation between the platform and China.³⁵

6.48 The AHRC argued that 'transparency is the key to ensuring that censorship (including extra-territorial censorship) does not unduly restrict the exercise of free speech in Australia' and therefore recommended that 'government should mandate that all social media platforms publicly disclose, in detail, all the content they censor and make it an offence to censor content where that has not been publicly disclosed to users'.³⁶

6.49 Twitter acknowledged in evidence to this committee that that such pressure from foreign governments had regularly occurred and had not been historically disclosed to its users:

Senator Chandler: What if it was an informal request [to take down or censor a tweet] from a government official? Would you let the user know who had made that request?

Mr Pickles: Historically, no. But this is actually one of the areas where we are looking to make significant changes to guard against the kind of pressure that the Twitter files disclosed that we as a service face.³⁷

6.50 Both Meta and Twitter referred to their transparency measures in place to report occasions where content is removed or restricted based on a legal request from a government or regulator. Meta advised the committee that it makes 'information transparently available relating to requests that we receive from all government around the world for content restrictions or requests for user data'.³⁸

6.51 Meanwhile, Twitter acknowledged that it may not be aware of all instances of requests to take down or censor content from officials acting on behalf of a foreign government:

Senator Chandler: What if the request to take down or censor a tweet was made by a foreign government? Would you let the user know that it was a foreign government making the request?

³⁴ Human Rights Watch, *Submission 12*, p. 8.

³⁵ Human Rights Watch, *Submission 12*, pp. 7–8.

³⁶ Australian Human Rights Commission, *Submission 9*, p. 16.

³⁷ Mr Nick Pickles, Twitter, *Committee Hansard*, 11 July 2023, p. 48.

³⁸ Meta, answers to written question on notice 1-11 (received 19 July 2023), p. 1–2.

Mr Pickles: If it came through a legal process, yes, we would. If it was someone in the Twitter app pressing a reporting button as a regular user, we might not know that person is from a foreign government. But in the case of a legal process – we receive thousands every year – we do communicate to the individual and actually provide them with a copy of the request as well.³⁹

6.52 The *Twitter files* referred to in Mr Pickles' evidence to the committee widely documents recent revelations from Twitter itself that governments and government staff often make informal or semi-formal requests or demands to staff at social media companies that content be censored or removed:

Slowly, over time, Twitter staff and executives began to find more and more uses for these tools. Outsiders began petitioning the company to manipulate speech as well: first a little, then more often, then constantly. By 2020, requests from connected actors to delete tweets were routine.⁴⁰

6.53 Both Meta and Twitter were unable to provide country level data on government requests outside of formal legal requests to remove or moderate content.

6.54 Meta did not directly address the question of whether it removes or restricts content for its users, including Australian users, following a request from a foreign government agency, regulator or official, where the content is **not a breach of local law** (emphasis added).⁴¹

6.55 Meta referred to its transparency report when asked whether Meta has ever acted on a request for content moderation on its platforms from the Russian Government, the Chinese Government or the Iranian Government or any persons connected to those regimes. However, those transparency reports only cite legal requests and not requests made through other informal channels.⁴²

6.56 Additionally, Meta's transparency report does not include data on content that they removed for violating their policies following a request from a foreign government: 'This report details instances where we restricted access to content based on local law. It does not include content that we removed for going against our policies'.⁴³

³⁹ Mr Nick Pickles, Twitter, *Committee Hansard*, 11 July 2023, p. 48.

⁴⁰ Matt Taibbi, *The Twitter Files*, 13 April 2023, <https://twitterfiles.substack.com/p/1-thread-the-twitter-files> (accessed 27 July 2023).

⁴¹ Meta, answers to written questions on notice 1-11 (received 19 July 2023), p. 1–2.

⁴² Meta, answers to written question on notice 1-11 (received 19 July 2023), p. 2–3.

⁴³ Meta, *Transparency Center: Content restrictions based on local law*, <https://transparency.fb.com/data/content-restrictions/> (accessed 27 July 2023).

6.57 Twitter was unable to provide detailed information about Australian Government agencies making requests to remove, restrict or limit the visibility of content that were not from a regulator acting to address an alleged breach of law.⁴⁴

6.58 While much of the public reporting on this issue focuses on pressure applied by United States (US) authorities to social media companies, companies acknowledge that similar requests outside of formal legal process are regularly made or attempted by foreign governments. When asked what processes are in place to ensure that Twitter's staff are not being target by foreign governments to action certain requests, Twitter told the committee:

Obviously, there are a number of different ways that foreign governments may target us as a company: through our employees is one and through our infrastructure is another. We have a corporate security team working across all of those threat vectors to keep Kathleen, me and our colleagues safe.⁴⁵

6.59 Social media companies have extensive flexibility within the application of their content rules to determine when content will, or won't be removed. Meta's Community Standards provides:

In some cases, we allow content – which would otherwise go against our standards – if it's newsworthy and in the public interest. We do this only after weighing the public interest value against the risk of harm, and we look to international human rights standards to make these judgments. In other cases, we may remove content that uses ambiguous or implicit language when additional context allows us to reasonably understand that the content goes against our standards.⁴⁶

6.60 Twitter acknowledged that pressure can be further amplified by overly broad and restrictive laws pressuring social media companies to remove or restrict content under poorly defined claims of 'misinformation' or 'social harm':

Globally, in pretty much every region and market we operate in, there is more regulation being proposed. In many countries, the legal definitions being proposed are so broad as to—I believe—pose a chilling risk to free expression. In some countries, it's phrases like 'harmful content'. Misinformation and disinformation are certainly concerns. We're seeing the pendulum swing towards more restrictive laws that don't necessarily have the same checks and balances or the ability to seek redress to the legal process that you would expect. Also, these decisions are being outsourced from governments to private companies to make the exact determination that you just talked about in terms of who decides whether content is illegal. Is it the state, or is it private companies? One trend we're definitely seeing is very broad laws being used to push that decision onto private companies

⁴⁴ Twitter, answers to written question on notice (received 25 July 2023), p. 1.

⁴⁵ Mr Nick Pickles, Twitter, *Committee Hansard*, 11 July 2023, p. 49.

⁴⁶ Meta, *Transparency Center: Facebook Community Standards*, <https://transparency.fb.com/en-gb/policies/community-standards/> (accessed 27 July 2023).

under threat of significant financial and, in some cases, criminal penalties. All of that will have a chilling effect on free speech.⁴⁷

Fact checking

- 6.61 The committee explored the issue whereby identifying misinformation and disinformation relies somewhat on common agreement on what information is factual and/or truthful. The role of fact-checking entities is discussed in greater detail in the chapter on civil society.
- 6.62 The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (Department of Communications) advised that under the proposed changes in the exposure draft of the Communications Legislation Amendment (Combating Misinformation and Disinformation) Bill 2023, 'the judgement or the determination of disinformation and misinformation on a digital platform is a responsibility that is being quite intentionally left in the hands of the digital platforms to manage themselves'.⁴⁸
- 6.63 Meta disagreed with that principle, stating that 'US based multinational technology companies should not necessarily be deciding some of these matters' and outlined that it invested in independent fact checkers, published transparency reports and has fact checks published on the fact-checker websites, 'so there can be debate around what content has been marked for removal or marked as false so that transparency can be applied across all of industry'.
- 6.64 Meta advised that the three firms it engages as fact checkers includes Australian Associated Press (AAP), Agence France-Presse (AFP) and RMIT FactLab and noted that all of them 'are accredited by the International Fact-Checking Network, which is the gold standard organisation of organisations that follow independent expert editorial approaches in the approach that they take to fact-checking'.⁴⁹
- 6.65 Meta explained that where the fact checking partner identifies false information, Meta does not remove the content but places a warning label over the content so people can click through and see the fact check statement. Meta noted that 'reasonable minds could disagree on what constitutes misinformation and we do not want to find ourselves in the position where we are making those

⁴⁷ Mr Nick Pickles, Twitter, *Committee Hansard*, 11 July 2023, p. 51.

⁴⁸ Mr Richard Windeyer, Deputy Secretary, Communications and Media Group, Department of Infrastructure, Transport, Regional Development, Communications and the Arts (Department of Communications), *Committee Hansard*, 12 July 2023, p. 26.

⁴⁹ Ms Mia Garlick, Meta, *Committee Hansard*, 11 July 2023, pp. 6 and 14.

judgements, so that's an area where we do treat speech a little differently, depending on who the speaker is'.⁵⁰

Job cuts

6.66 The Department of Communications noted that recent job cuts are an emerging concern for the ability of digital platforms to respond to and counter foreign interference. It further noted that the Australian Government expects digital platforms to still fulfil their commitments under the DIGI Code:

Twitter, Meta, Google, TikTok, Snap, Microsoft and Amazon have all announced significant job cuts, with Apple pausing almost all new hiring. This raises questions about the impact of job cuts on Australian based staff, and moderation, safety, policy and government engagement teams globally. Media reporting indicates that these cuts have impacted moderation and safety teams at some platforms, e.g. job cuts at Twitter have affected about 15 percent of its Trust and Safety Group globally and most of its Australian staff working on public policy and safety issues.⁵¹

6.67 Human Rights Watch submitted that in the past, Twitter had responded quickly to requests to protect the accounts of the Chinese human rights defenders, but stated there is a chance after the recent ownership changes that a reduction in staff numbers 'threatens to change that equation between the platform and China'.⁵²

6.68 Twitter responded to these allegations directly to the committee, stating:

Contrary to media reporting, when the restructuring was happening the trust and safety team was affected disproportionately less compared to other teams in the company. You'll have heard our new owner speaking about the importance of content moderation and the importance of preventing manipulation. Indeed, he's spoken about how one of the primary motivators for purchasing the company was preventing manipulation.⁵³

Transparency

6.69 Transparency, or rather the lack of it, was raised consistently by many organisations and expert witnesses as an issue of key concern. Transparency issues were raised across many different domains, such as transparency in reporting content removal, recommender algorithms and actions taken against coordinated inauthentic behaviour.

6.70 In relation to transparency through reporting, Meta submitted that it reports regularly on its approach to CIB through quarterly *Community Standards*

⁵⁰ Mr Josh Machin, Head of Public Policy, Australia, Meta, *Committee Hansard*, 11 July 2023, p. 11.

⁵¹ Department of Communications, *Submission 7*, p. 3.

⁵² Human Rights Watch, *Submission 12*, pp. 7–8.

⁵³ Mr Nick Pickles, Twitter, *Committee Hansard*, 11 July 2023, p. 41.

*Enforcement Reports, Monthly Adversarial Threat Reports, and via the Threat Report—State of Influence Operations 2017–2021.*⁵⁴

- 6.71 Twitter told the committee that its transparency reporting was under review, particularly in relation to disclosures, because 'some of the impacted states were reacting with hostility towards both our company and our employees, so we were also starting to face challenges around how we could do that work safely'.⁵⁵
- 6.72 AHRC recommended that one aspect of transparency should be that platforms are required to publicly disclose the content that they censor and it should be made an offence 'to censor content where that has not been publicly disclosed to users'. AHRC argued this measure would help to ensure that censorship (including extraterritorial censorship) does not unduly restrict the exercise of free speech in Australia.⁵⁶
- 6.73 ASPI made a broader recommendation, that there should be an 'explicit social contract ... mandating social media platforms to disclose state-backed influence operations and other transparency reporting to increase public awareness'.⁵⁷
- 6.74 Meta and Twitter noted they have transparency measures to report where content is removed or restricted based on a legal request from a government or regulator, but noted they might not always know when a request is from a government actor. Mr Nick Pickles of Twitter told the committee:
- If it was someone in the Twitter app pressing a reporting button as a regular user, we might not know that person is from a foreign government.⁵⁸
- 6.75 Mr Pickles acknowledged pressure from some governments not to disclose that a content removal request had been made, and noted that strengthened transparency requirements would be a protective factor against such pressure:
- I think transparency is a phenomenal deterrent for pressure being applied. If a government knows that their request may be [relayed] to the individual, that makes the people submitting that request consider whether they want to do so.⁵⁹
- 6.76 Meta pointed to its transparency reports indicating that users can view content restrictions as a result of government requests. However, if a government request cites a breach of Meta's content policies, the request is not reported

⁵⁴ Meta, *Submission 32*, pp. 15–16.

⁵⁵ Mr Nick Pickles, Twitter, *Committee Hansard*, 11 July 2023, p. 42.

⁵⁶ Australian Human Rights Commission, *Submission 9*, p. 16.

⁵⁷ Australian Strategic Policy Institute, *Submission 13*, p. 13.

⁵⁸ Meta, answers to written questions on notice (1-11) 11 July 2023 (received 19 July 2023); Mr Nick Pickles, Twitter, *Committee Hansard*, 11 July 2023, p. 48.

⁵⁹ Mr Nick Pickles, Twitter, *Committee Hansard*, 11 July 2023, p. 48.

coming from a government, skewing the overall numbers of removal requests attributed to governments or state-actors.⁶⁰

- 6.77 ASPI noted the lack of transparency from TikTok in relation to removed networks on its app:

When you look at TikTok's disclosures, there is a claim that a network was taken down, but there is no information about what type of content it had, how it was done or any other information to actually verify and check to make sure they're not just silencing voices. For example, they took down a network operating out of Taiwan but didn't disclose what conversations or what topics those accounts were disclosing. That's concerning from an individual perspective, if the platform are taking down content or campaigns without giving a justification, as to whether it is proportional to the campaign itself. It's an important democratic principle to hold powerful platforms to account and do it transparently.⁶¹

- 6.78 Mr David Robinson, Director of Internet 2.0, noted that transparency around how companies make decisions was critical for individuals to make informed decisions:

Consumers, in the end, will look at the risk-reward situation of their data and make decisions. But, if they can't make decisions because there's no transparency, then the first step in the process is pretty hard to do.⁶²

- 6.79 Ms Yaqiu Wang of Human Rights Watch argued there is a role for governments to 'force companies to be transparent about what they are censoring, what they are suppressing, what they are promoting' and said this could be done without adversely affecting how people use apps.⁶³

- 6.80 However, Meta noted that in relation to foreign interference 'it may not always be appropriate to have immediate transparency about steps taken to combat foreign interference. There are sometimes very good national security reasons why there may be a delay on that particular type of information, as I suspect security agencies may have advised this committee'.⁶⁴

- 6.81 To address this, Meta advised the committee it has created partnerships with a handful of security expert organisations, which are given information that is not publicly available, such as ASPI. It noted that:

⁶⁰ Mr Josh Machin, Meta, *Committee Hansard*, 11 July 2023, p. 10; Meta, *Content restrictions based on local law*, <https://transparency.fb.com/data/content-restrictions/> (accessed 26 July 2023).

⁶¹ Mr Albert Zhang, Analyst, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 21.

⁶² Mr David Robinson, Director, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 35.

⁶³ Ms Yaqiu Wang, Senior China Researcher, Human Rights Watch, *Committee Hansard*, 21 April 2023, p. 2.

⁶⁴ Mr Josh Machin, Meta, *Committee Hansard*, 11 July 2023, p. 7.

... we will provide them with more detailed information about our take-downs than is available in the adversarial threat reports so that that can inform a lot of their research reports that they then provide publicly to the intelligence community about trends and patterns.⁶⁵

6.82 The AHRC recommended the Australian Government should 'establish clear and mandatory requirements and pathways for social media organisations to report suspected foreign interference activities'.⁶⁶

6.83 ASPI recommended 'regulation or at least a discussion about how we standardise and create better reporting mechanisms to increase transparency'.⁶⁷

6.84 Meta agreed with ASPI on this, and stated that 'there has not been a benchmarking exercise or a standardisation of the metrics across all the companies that are signatories [to the code]'.⁶⁸ Meta pointed to a global organisation called the Digital Trust & Safety Partnership, which is conducting 'a really deep-dive project particularly on this topic, about how you design transparency in ways to actually make it effective'. Meta suggested the outcomes of this project could be 'an important contributing factor to what the ACMA and policymakers might want to have in place as part of legislative reform in Australia'.⁶⁹

6.85 The ACMA similarly noted that:

We think there is still a way to go in terms of those reports. There's still very limited information about how platforms are going about measuring the effectiveness and impact of the measures they're reporting on under the outcomes of the code, and there is a lack of consistency. So, at the moment, we're not in a position to be able to assess, if you like, how measures that one signatory might be doing look against the impact of similar measures a different signatory might be doing.⁷⁰

6.86 However, the ACMA did acknowledge some improvements it had seen in reporting on Australian-specific data relating to misinformation, disinformation and CIB.⁷¹

⁶⁵ Ms Mia Garlick, Meta, *Committee Hansard*, 11 July 2023, p. 9.

⁶⁶ Australian Human Rights Commission, *Submission 9*, p. 8.

⁶⁷ Mr Albert Zhang, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 21.

⁶⁸ Mr Josh Machin, Meta, *Committee Hansard*, 11 July 2023, p. 7.

⁶⁹ Mr Josh Machin, Meta, *Committee Hansard*, 11 July 2023, p. 8.

⁷⁰ Ms Cathy Rainsford, Australian Communications and Media Authority, *Committee Hansard*, 12 July 2023, pp. 27–28.

⁷¹ Ms Cathy Rainsford, Australian Communications and Media Authority, *Committee Hansard*, 12 July 2023, pp. 27–28.

Partnerships with civil society

6.87 The committee heard that partnerships between platforms and civil society were an important risk amelioration tool. These could be ongoing partnerships, such as fact-checking services, or could simply be that platforms provide the data necessary for expert organisations to undertake their research on foreign interference issues. However, while some platforms currently had such partnerships, there were ongoing concerns how effective they were, particularly in relation to data sharing.

6.88 Meta outlined it was a major sponsor of the ASPI, which is among the small group of researchers it shares information with about CIB takedowns. Meta also funded an ASPI review of information-for-hire, focused on the Asia-Pacific region.⁷²

6.89 Dr Andrew Dowse, Director of RAND Australia noted how difficult it is for researchers to identify incidents of foreign interference. Without access to social media networks' internal identification data, researchers have to attempt to identify patterns in data and noted the need for greater funding:

There are limited funding sources being provided in these areas. So in general we in RAND have been utilising US studies and US funding to be able to do it. I would dearly like to see the Australian government perhaps providing more sources of funding so we can do this research. At the moment all the research we've done in this area in Australia from a RAND perspective has been internally funded.⁷³

6.90 Professor Rory Cormac from the University of Nottingham noted the need for greater research to understand the scope of the problem, noting that states tend to count only in metrics—how many people were reached, or how many inauthentic newspaper articles were placed. Professor Cormac advised that this 'gives a misleading idea of the impact, because it doesn't tell you what the scope and the scale were'. Professor Cormac went on to detail some of the analysis that is required:

Sometimes [states] work through legitimate actors. Sometimes they work through what were once called unwitting idiots. Sometimes they work through stooges. Sometimes they work through local influencers. So there's a whole spectrum, and we need to map that spectrum, that relationship between the state and the non-state actor or the conduit, to get a good sense of how direct or indirect this data is in order for us to counter that.⁷⁴

6.91 Professor Cormac later expanded on this and noted the need for greater analysis of the impacts of CIB:

⁷² Meta, *Submission 32*, p. 15.

⁷³ Dr Andrew Dowse, Director, RAND Australia, *Committee Hansard*, 20 April 2023, p. 28.

⁷⁴ Professor Rory Cormac, Director, Centre for the Study of Subversion, Unconventional Interventions and Terrorism, University of Nottingham, *Committee Hansard*, 20 April 2023, p. 37.

It's not enough for us as governments to know how many people clicked on that. We then need to know: what did they do next? Did they click on Russian propaganda or terrorist propaganda or Chinese propaganda? Did they then get radicalised? Did they then click on something else? What was their journey? Being able to master that—that's big data and that's tough. That kind of behavioural change as a consequence needs to be measured.⁷⁵

- 6.92 Dr Stoltz advised that this approach would best be done in collaboration with classified intelligence collection to understand the intent of adversaries, so that 'we are informed through potentially classified information about what the core strategic intent of the adversary is, it means that our response can be managed in a more proportionate way and we don't get stuck in a loop of misunderstanding and reacting in inappropriate ways that causes a kind of escalation cycle'.⁷⁶
- 6.93 Twitter flagged that it was open to an approach for providing data to academics where researchers could be 'accredited by governments, in some cases, or public institutions, as a form of vetting to actually protect the data itself from bad actors'.⁷⁷ Meta submitted that its ThreatExchange application programming interface (API) facilitates industry efforts to combat cyberthreats, through the threat signal sharing between security professionals.⁷⁸
- 6.94 Professor Cormac noted that to improve access to necessary data for analytical research, there had to be an international response. Governments could work together to persuade firms to share the data, either through the United Nations General Assembly, or via smaller groupings such as the Quadrilateral Security Dialogue (the Quad), the Association of Southeast Asian Nations (ASEAN) or 'or any other combination of multilateral groupings, in order to try and create cross-jurisdictional norms and standards that we're satisfied with, and then we can generate that scale to bring these companies into an alignment with an obligatory regime rather than one that is solely voluntary'.⁷⁹

Unverified accounts

- 6.95 Anonymity was also discussed as a concern. In regard to anonymity and identity shielding, this has benefits in that they can protect users' privacy, but they can also be weaponised to enable foreign interference. Some platforms' verification processes—or lack of—allow for fake, imposter, or multiple

⁷⁵ Professor Rory Cormac, University of Nottingham, *Committee Hansard*, 20 April 2023, p. 41.

⁷⁶ Dr William Stoltz, Private capacity, *Committee Hansard*, 20 April 2023, p. 41.

⁷⁷ Mr Nick Pickles, Twitter, *Committee Hansard*, 11 July 2023, pp. 42–43.

⁷⁸ Meta, *Submission 32*, p. 15.

⁷⁹ Professor Rory Cormac, University of Nottingham, *Committee Hansard*, 20 April 2023, p. 42.

accounts to be created and operated by one user, which can then be used to conduct online foreign interference activities in an unmoderated way.⁸⁰

- 6.96 Dr Andrew Dowse noted that allowing unverified accounts exacerbates the dangers of foreign interference via social media.⁸¹

Platforms and authoritarian states

- 6.97 Many submitters and witnesses stressed that platforms which originate from authoritarian states pose additional security concerns that are not applicable to platforms that operate under free market principles within a liberal democracy. In particular, discussions centred on TikTok and WeChat.⁸²

- 6.98 CyberCX warned the committee that the collection and aggregation of the personal information of millions of Australians and the capacity for malign foreign actors to manipulate content consumed by Australians at scale is a heightened risk when using platforms that are linked to authoritarian governments, including TikTok and WeChat. As CyberCX pointed out, Chinese corporations are required by Chinese law to cooperate with Chinese government authorities which operate 'without the oversight and transparency mechanisms of rule-of-law democracies'.⁸³

- 6.99 ASIO highlighted the additional security concerns that authoritarian governments 'are able to direct their country's institutions—including media, businesses and society—to support intelligence or foreign policy objectives in ways which are not acceptable in a democracy'.⁸⁴

- 6.100 Internet 2.0 likewise argued that the 'free market principles' under which we allow companies to operate in a liberal democracy should not extend to authoritarian-based companies:

They should not be allowed to gain profit and capital at the expense of our national security. Ultimately, they do not reside in our society. Social media companies that reside in our society will contribute and attempt to uphold democratic values. These companies should be defended against social media companies that align with our authoritarian competitors, because

⁸⁰ Australian Security Intelligence Organisation, *Submission 2*, p. 5.

⁸¹ Dr Andrew Dowse, RAND Australia, *Committee Hansard*, 20 April 2023, p. 28.

⁸² See, for example: Dr Seth Kaplan, *Committee Hansard*, 20 April 2023, p. 13; Mr Fergus Ryan, Analyst, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, pp. 19, 21–22; Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 31; US Federal Communications Commission, *Submission 4*, p. 2; Australian Strategic Policy Institute, *Submission 13*, pp. 7–11; Rachel Lee, Prudence Luttrell, Matthew Johnson, John Garnaut, *Submission 34*, pp. 3–5.

⁸³ CyberCX, *Submission 16*, p. 5.

⁸⁴ Australian Security Intelligence Organisation, *Submission 2*, p. 4.

they flourish only as a result of our free-market principles and democratic system.⁸⁵

6.101 Ms Shanthi Kalathil, a former advisor on the US National Security Council, told the committee that these platforms are increasingly the propaganda tool of choice of authoritarian states:

... network cross-border influence operations by authoritarian actors have grown in sophistication and effectiveness in recent years, shaping narratives and targeting democratic institutions during important geopolitical moments. These include but are certainly not limited to election periods. While not disavowing more traditional forms of propaganda, authoritarian regimes are increasingly using digital influence operations as a method of censorship and manipulation, flooding the information space with false or misleading narratives designed to crowd out independent voices and expertise.⁸⁶

6.102 Ms Kalathil further advised the committee that 'we should not simply examine authoritarian links to social media platforms; we should put them in the context of the history and political systems from which they emerged, particularly with respect to the legacy of how those systems understand and manage information' and noted that the implications of data collection by those authoritarian states was concerning, particularly in light of their security agencies attempting to harness big data for predictive policing.⁸⁷

6.103 ASPI used the above approach and put TikTok and ByteDance into their political context, by reminding the committee of the obedience to the CCP forced upon the ByteDance founder:

For TikTok's parent company ByteDance, this authoritarian approach has included compelling the company's founder Zhang Yiming to make an abject apology in a public letter for failing to respect the Chinese Communist Party's 'socialist core values' and for 'deviating from public opinion guidance'—one of the CCP's terms for censorship and propaganda.⁸⁸

6.104 ASPI advised the committee that this poses a regulatory challenge for government, such that platforms originating from authoritarian states do not face the same oversight in their home nations:

Policymakers and legislators should ensure that when addressing the social media challenges (and broader technology risks) they do not disproportionately regulate Western technology platforms while ignoring technology platforms that originate from China or Russia. Democracies must not exacerbate the already unlevel playing field when our ultimate

⁸⁵ Internet 2.0, *Submission 17*, p. 3.

⁸⁶ Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, pp. 1–2.

⁸⁷ Ms Shanthi Kalathil, *Committee Hansard*, 20 April 2023, p. 2.

⁸⁸ Australian Strategic Policy Institute, *Submission 13*, p. 10.

objective is to be able to compete against the authoritarian regimes which are abusing technology to further their strategic interests.⁸⁹

6.105 In relation to WeChat, Dr Seth Kaplan, a US political expert, argued that platform is 'basically a narrative machine for the CCP and what it wants to promote'.⁹⁰ WeChat remains a wholly-owned subsidiary of Tencent with its headquarters in Shenzhen, China.⁹¹

6.106 Much is made about the importance of the WeChat platform to Chinese-heritage Australians:

WeChat is essential to communication between Chinese Australians and their families, friends, and business partners in China. This is largely due to the fact that social media platforms such as WhatsApp and Facebook are not allowed in China. WeChat is a necessity, not a choice for many Chinese Australians.⁹²

6.107 Professor Wanning from the Australia-China Relations Institute (ACRI) at the University of Technology Sydney and Professor Haiqing, Professor of Media and Communications at RMIT, argued against the notion that the WeChat platform is heavily censored in favour of the CCP, submitting 'WeChat, like Facebook and Twitter, is a social media platform that carries wide-ranging and diversely sourced content; its ideological landscape is fragmented and contested'.⁹³ ACRI's founding donor and chairman, Huang Xiangmo, was later banned from Australia on national security grounds.⁹⁴

6.108 The artist Badiucaio disagreed and noted that because of the way WeChat operates in Australia, it enables the Chinese government 'to export its censorship outside of China regardless of local law or rights protection in Australian society'.⁹⁵

6.109 The Australian Electoral Commission (AEC) noted that although it monitors social media platforms as part of its work on election integrity, it does not monitor WeChat in the same way, because much of the conversation in WeChat occurs in closed channels. The AEC noted that on other platforms it also only

⁸⁹ Australian Strategic Policy Institute, *Submission 13*, p. 7.

⁹⁰ Dr Seth Kaplan, *Committee Hansard*, 20 April 2023, p. 12.

⁹¹ Social media users in China use Weixin, operated by a Chinese entity and governed by Chinese law. WeChat in Australia is designed for users outside of mainland China.

⁹² Professor Sun Wanning and Professor Yu Haiqing, *Submission 37*, p. 2.

⁹³ Professor Sun Wanning and Professor Yu Haiqing, *Submission 37*, p. 2.

⁹⁴ Nick McKenzie and Chris Uhlmann, ['Canberra strands Beijing's man offshore, denies passport'](#), *The Sydney Morning Herald*, 5 February 2019; James Leibold, ['The Australia-China Relations Institute doesn't belong at UTS'](#), *The Conversation*, 5 June 2017.

⁹⁵ Badiucaio, Private capacity, *Committee Hansard*, 21 April 2023, p. 35.

monitors comments made in open channels, and it does not monitor individual conversations.⁹⁶

- 6.110 In relation to TikTok, warnings regarding the security of the platform have come from a variety of sources for many years. Most recently, in May 2023 the former head of engineering for ByteDance's US operations, Yintao Yu, alleged TikTok served as a propaganda tool for the Chinese government by suppressing or promoting content favourable to the country's interests. Mr Yu alleged the Chinese government monitored ByteDance's work from within its Beijing headquarters and provided guidance on advancing 'core communist values' and maintained access to all company data, including information stored in the US.⁹⁷
- 6.111 In response to concerns around the platform, on 4 April 2023, the Australian Attorney-General, The Hon Mark Dreyfus KC MP, banned TikTok from being installed on government devices, except in limited circumstances. The ban has been implemented at a government level in other western countries including the US, the United Kingdom (UK), New Zealand, Canada and France.⁹⁸
- 6.112 The main concerns are China's national security law coupled with the data TikTok collects on its users. The 2017 law requires organisations and citizens to 'support, assist and cooperate with the state intelligence work', with experts saying while there is no definitive proof that China's government has used this law with TikTok, the type of data TikTok collects makes this a high risk.⁹⁹
- 6.113 The following sections outline some of the specific concerns with platforms such as TikTok and WeChat.

CCP national security laws

- 6.114 A key concern raised regarding platforms that originate from authoritarian states such as China, was that the data collected by those apps from millions of Australians can be misused to create targeted foreign interference

⁹⁶ Mr Tom Rogers, Electoral Commissioner, Australian Electoral Commission, *Committee Hansard*, 12 July 2023, pp. 34–35.

⁹⁷ ['Executive fired from TikTok's parent company ByteDance lays complaint against tech giant'](#), ABC News, 13 May 2023, Haleluya Hadero, ['Fired TikTok exec says Chinese government had access to app user data'](#) Sydney Morning Herald, 13 May 2023.

⁹⁸ The Hon Mark Dreyfus KC MP, ['TikTok ban on Government devices'](#), Media release, 4 April 2023; Josh Taylor, ['What does TikTok's ban from Australian government devices mean for its future?'](#), The Guardian, 4 April 2023.

⁹⁹ Josh Taylor, ['What does TikTok's ban from Australian government devices mean for its future?'](#), The Guardian, 4 April 2023. See, for example: Simon Jiandan, *Submission 36*, pp. 1, 3 and 8; US Federal Communications Commission, *Submission 4*, pp. 1–5; AHRC, *Submission 9*, pp. 13–14; Rachel Lee, Prudence Luttrell, Matthew Johnson, John Garnaut, *Submission 34*, pp. 67–71.

campaigns.¹⁰⁰ Many submitters and witnesses noted that Chinese national security and data laws meant that private companies are required by Chinese law to assist national security agencies with any request they may make, and furthermore, that those requests must be kept secret. Ms Shanthi Kalathil stated:

... I believe the structure of the party state in the People's Republic of China is such that, were the party to make demands on private companies, there's no legal or technical way for those companies to resist those demands.

...

I would also say those companies in particular that you mentioned [Tencent and ByteDance] have already been named as particular champions by the state. They been designated as having a special relationship with the state, so they are in a bit of a different category; they are not like some of the smaller ones. Their entwinement and entanglement not just with the state but with the military and with overarching state priorities puts those companies in a special category.¹⁰¹

6.115 Ms Kalathil further noted that large companies such as ByteDance and Tencent are required to have CCP cells operating within them.¹⁰²

6.116 ASPI noted of TikTok that:

The enormous leverage that the CCP has over the company is what drove the company at the time to boost its army of censors by an extra 4,000 people (candidates with party loyalty were preferred) and it's what continues to motivate ByteDance to conduct 'party-building' exercises inside the company.¹⁰³

6.117 Internet 2.0 noted further dangers that platforms such as TikTok and WeChat pose:

We assess that social media companies which reside in our authoritarian competitors' orbit will not act in our democratic interests; if we attempt to compel them to remove disinformation, they can resist this as they balance the competing interests of the authoritarian regime. They can resist our sovereign interventions by hosting data, media, and their platforms outside of our jurisdiction.¹⁰⁴

6.118 When asked about these Chinese national security laws and the safety of TikTok data from being shared with the CCP, the Australian Signals Directorate advised

¹⁰⁰ CyberCX, *Submission 16*, p. 5.

¹⁰¹ Ms Shanthi Kalathil, *Committee Hansard*, 20 April 2023, p. 3. See also: Simon Jiandan, *Submission 36*, p. 8; Human Rights Watch, *Submission 12*, pp. 2–3; Internet 2.0, *Submission 17 Attachment 1*, p. 10.

¹⁰² Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, p. 3.

¹⁰³ Australian Strategic Policy Institute, *Submission 13*, p. 10.

¹⁰⁴ Internet 2.0, *Submission 17*, p. 6.

the committee that it had 'not seen technical controls that would provide a basis for technical advice that the risks of sharing data are adequately mitigated'.¹⁰⁵

6.119 Furthermore, ASIO advised that 'like any individual in a corporation or in government, if they [employees] have access to sensitive information or if they have the ability to propagate foreign interference, there will always be the potential that they'll be targeted'.¹⁰⁶

6.120 Ms Yaqui Wang of Human Rights Watch also expressed doubt that companies like Tencent and ByteDance would not share data when asked by the CCP because 'their livelihood is hinged to the Chinese Communist Party'.¹⁰⁷

6.121 Ms Lindsay Gorman of the Alliance for Securing Democracy advised the committee that:

Our research has found that, despite the professed separation between the CCP and TikTok, PRC diplomats and state media accounts have gone to bat to TikTok, with messaging campaigns designed to paint the app in a benign light, hype up TikTok's popularity and the consequences of the ban, denigrate the US political system as hostile to business, and portray criticism of TikTok or China as xenophobic, often drawing on familiar tropes.¹⁰⁸

6.122 Ms Ella Woods-Joyce, Acting Director of Public Policy, Australia and New Zealand, TikTok, argued that TikTok Australia has 'never been asked for that user data and we would not provide it if we were asked'. Ms Woods further argued that data is not stored in China but did concede that did not mean data was not retrievable from China, as China based TikTok employees have access to data stored outside of China.¹⁰⁹

6.123 The claim that TikTok would not provide data was not seen as credible by many inquiry participants.¹¹⁰ Mr Brendan Carr, one of three United States Federal Communications Commissioners, noted that:

¹⁰⁵ Ms Abigail Bradshaw, Deputy Director-General, Australian Signals Directorate, *Committee Hansard*, 12 July 2023, p. 3.

¹⁰⁶ Mr Mike Noyes, Deputy Director-General, Intelligence Service Delivery, Australian Security Intelligence Organisation, *Committee Hansard*, 12 July 2023, p. 8.

¹⁰⁷ Ms Yaqui Wang, Human Rights Watch, *Committee Hansard*, 21 April 2023, p. 3.

¹⁰⁸ Ms Lindsay Gorman, Senior Fellow for Emerging Technologies, Alliance for Securing Democracy, German Marshall Fund, *Committee Hansard*, 21 April 2023, p. 8.

¹⁰⁹ Ms Ella Woods-Joyce, Acting Director of Public Policy, Australia and New Zealand, TikTok, *Committee Hansard*, 11 July 2023, pp. 22 and 23; TikTok, answers to questions on notice (4, 5, 6), 11 July 2023 (received 21 July 2023).

¹¹⁰ For example, see: Human Rights Watch, *Submission 12*, pp. 6–8; Internet 2.0, *Submission 17 Attachment 1*, p. 10; Rachel Lee, Prudence Luttrell, Matthew Johnson, John Garnaut, *Submission 34*, p. 44, 47, 53 and 60–62.

The argument that somehow TikTok are going to stand up to the CCP is belied by their inability to do it at any point in time publicly. For instance, they've been asked in US media interviews whether they acknowledge the existence of the Uighur genocide that's taking place in Xinjiang. Their official on TV refused to address it. That same question was posed to their CEO when he testified here recently, and once again he declined to address it. If a TikTok official is not willing to say that the CCP is committing genocide with respect to Uighurs then that gives very little comfort that they would turn them down and say no to them when they do come to them for access. And it's almost separate from access; they're so intermingled here right now in terms of the data that is accessible from inside China, it's not clear that a formal ask would even be necessary in these circumstances.¹¹¹

6.124 TikTok Australia did concede that it has engineers located within China who are working on the TikTok app, and further, that those workers were not under the direction or control of Mr Lee Hunter, the General Manager of Operations for TikTok Australia. It was later acknowledged that staff located in mainland China where the Chinese national security and data laws operate, do indeed have access to Australians' data that is harvested by the TikTok app, and can also make changes to the operation of the algorithm which influences what users see.¹¹²

6.125 Mr Hunter, despite having made assurances that Australian TikTok users' data is safe, also acknowledged that he is just 'one of several spokespeople for TikTok in Australia' and that he relies on the expertise of others to ensure his statements are factually accurate.¹¹³

Use of data TikTok data for CCP purposes

6.126 Numerous reports exist that data collected by TikTok has made it into the hands of the CCP and has been put to use for political harassment and interference. For example, the AHRC submitted that 'ByteDance had used TikTok to track the physical location of multiple Forbes journalists who were reporting on the company as part of a covert surveillance campaign' and an 'investigation by BuzzFeed News that concluded China-based TikTok employees had access to US user data, and repeatedly accessed that data'.¹¹⁴

6.127 Mr Hunter, discussed the allegations of surveillance when they first arose, in an opinion piece in the *Daily Telegraph* newspaper on 24 October 2022, stating that:

¹¹¹ Mr Brendan Carr, Commissioner, United States Federal Communications Commission, *Committee Hansard*, 20 April 2023, p. 7.

¹¹² Ms Ella Woods-Joyce, TikTok, *Committee Hansard*, 11 July 2023, p. 22 and Mr Lee Hunter, General Manager, Operations, Australia and New Zealand, TikTok, *Committee Hansard*, 11 July 2023, p. 25.

¹¹³ Mr Lee Hunter, TikTok, *Committee Hansard*, 11 July 2023, p. 25.

¹¹⁴ Australian Human Rights Commission, *Submission 9*, p. 13.

Unfortunately, some of the public criticism TikTok has faced recently has not been based on fact but exaggeration, speculation and sometimes pure fabrication.

Take for example a recent report that suggested 'TikTok parent ByteDance planned to use TikTok to monitor the physical location of specific American citizens'.

The fact is ... TikTok has never been used to 'target' any members of the US government, activists, public figures or journalists, nor do we serve them a different content experience than other users.

TikTok does not collect precise GPS [Global Positioning System] location information from US (or Australian) users, meaning TikTok could not monitor US users in the way the article suggested.¹¹⁵

6.128 Later when discussing the case with the committee, Mr Hunter said he disputed 'the characterisation that we spied on journalists' and claimed it was the actions of 'rogue employees [who] are no longer with the business'. Mr Hunter informed the committee that strengthened policies meant this could not happen again, however, he did not acknowledge that in October 2022 he had declared the breach was not technically possible, and that 'TikTok could not monitor US users in the way the article suggested'.

6.129 Mr Hunter did not respond to questions from the committee as to why he should be believed this time—given he had previously declared the breach could not occur and was proven wrong—and as to why he did not seek to correct the record. Mr Hunter's evidence to the committee lacked credibility and candour.¹¹⁶

6.130 Ms Woods-Joyce of TikTok Australia also discussed the current court case in which former employees disclosed that TikTok used its data to spy on users in Hong Kong, stating that 'we will be contesting the range of allegations that has been made in that matter'.¹¹⁷

6.131 US Federal Communications Commissioner Brendan Carr told the committee that TikTok 'presents an exceedingly unique threat to national security' for two reasons, being surveillance and foreign influence. Commissioner Carr noted that in relation to surveillance 'TikTok operates as a very sophisticated surveillance technology' and while TikTok claims it collects very little data:

... that's not what the evidence indicates. TikTok collects everything from search and browsing history to keystroke patterns, and its terms of service reserve the right to get biometrics, including face prints and voice prints. For years, TikTok told regulators not to worry and that the data was not stored

¹¹⁵ Lee Hunter, ['TikTok boss Lee Hunter asks for be measured on fact not fiction'](#), *Daily Telegraph*, 24 October 2022.

¹¹⁶ Mr Lee Hunter, TikTok, *Committee Hansard*, 11 July 2023, pp. 24–25.

¹¹⁷ Ms Ella Woods-Joyce, TikTok, *Committee Hansard*, 11 July 2023, p. 30.

inside China. In some places it said that the data didn't even exist inside China.

Flash forward to this past summer, and a BuzzFeed News report got internal TikTok communications that showed that in fact everything 'is seen inside China'. We've seen additional evidence pile on from there. For instance, TikTok denied a report that it—a China based team—was using the app to surveil the location of specific Americans. It said that that report lacked journalistic integrity. It turns out that that report was entirely accurate, and TikTok has now admitted that it used the app to surveil the locations of specific Americans—in fact, reporters that have been writing negative stories about TikTok and other reporters located outside the United States as well. Now the US Department of Justice and FBI [US Federal Bureau of Investigation] are looking into that exact type of conduct.¹¹⁸

6.132 ASPI expressed similar concerns, citing data security and content manipulation, further noting that the leverage the CCP has over TikTok 'exacerbates the former two risks and is unique to TikTok as a major mainstream social media app'.¹¹⁹

6.133 Internet 2.0 has conducted an in-depth analysis of the TikTok application and the data it collects, and found that:

We've conducted code analysis on their location data twice, first last year and then secondly about two months ago. Their code basically accesses coarse and fine location and has a specific 'get long get lat' string that in essence basically pulls the longitude and latitude from the GPS into the app. TikTok queries that location data specifically. The accuracy is debatable, but that's a technical discussion about whether it's five metres accurate or 20 metres accurate. The fact that they actually pull the location is still there. It's another example of the lack of transparency and confusing response from TikTok, in my opinion. We just printed the code location requests and then they denied it. We said, 'This is a picture.' Anyway, they updated their code in the last six months. Previously they could get basically a horizontal and vertical location on the map. But they have updated their location data when we last analysed it, so now they can get bearing, speed and altitude. So if you're in a high-rise building, they can tell what floor you're on now. That wasn't previously in their code, last year.¹²⁰

6.134 David Robinson of Internet 2.0 advised that 'we saw no reason, in order to create an effective video platform, to have all that data' and compared the practice to that of YouTube and Instagram, which are less invasive.¹²¹ Mr Robinson noted that:

¹¹⁸ Mr Brendan Carr, United States Federal Communications Commission, *Committee Hansard*, 20 April 2023, p. 6.

¹¹⁹ Mr Fergus Ryan, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 18.

¹²⁰ Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 32.

¹²¹ Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 32.

On an even basis, with a transparency scoring system, TikTok is the worst app that we have published in social media.¹²²

- 6.135 In response, Ms Woods-Joyce of TikTok said that the report contains 'a range of information that is not necessarily accurate' but was not specific as to what she claimed was not correct.¹²³

Manipulation of content algorithms

- 6.136 Another concern raised by inquiry participants was the use of TikTok by the CCP to further its propaganda, including through the manipulation of content algorithms or 'heating' buttons.

- 6.137 In relation to foreign influence, Commissioner Carr noted that:

... the CCP's propaganda arm set up TikTok accounts and, unlike other social media, did not disclose the state media affiliation of those accounts. Those accounts targeted US politicians for criticism ahead of our most recent mid-term elections—accounts that saw millions and millions of views on those videos.¹²⁴

- 6.138 Ms Lindsay Gorman of the Alliance for Securing Democracy noted that 'TikTok's heating button, for example, reportedly allows employees to manually make specific content go viral' and further noted that if the CCP were to direct TikTok to heat certain content, 'it would be extremely difficult to discern this manipulation'.¹²⁵

- 6.139 ASPI submitted that leaked documents have revealed that TikTok instructed moderators to censor videos that 'mention Tiananmen Square, Tibetan independence, or the banned religious group Falun Gong'. TikTok conceded this occurred but insisted 'those documents don't reflect its current policy and that it had since embraced a localised content moderation strategy tailored to each region'.¹²⁶

- 6.140 ASPI further noted that:

In 2022, TikTok blocked an estimated 95% of content previously available to Russians, according to Tracking Exposed, a nonprofit organization in Europe that analyses algorithms on social media. In addition to this mass restriction of content, the organisation also uncovered a network of coordinated accounts that were using a loophole to post pro-war propaganda in Russia on the platform. In other words, at the outset of

¹²² Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 33.

¹²³ Ms Ella Woods-Joyce, TikTok, *Committee Hansard*, 11 July 2023, p. 25.

¹²⁴ Mr Brendan Carr, United States Federal Communications Commission, *Committee Hansard*, 20 April 2023, p. 6.

¹²⁵ Ms Lindsay Gorman, Alliance for Securing Democracy, *Committee Hansard*, 21 April 2023, p. 8.

¹²⁶ Australian Strategic Policy Institute, *Submission 13*, p. 9. See also: Ms Ella Woods-Joyce, TikTok, *Committee Hansard*, 11 July 2023, pp. 29–30.

Putin's invasion of Ukraine, TikTok was effectively turned into a 24/7 propaganda channel for the Kremlin.¹²⁷

- 6.141 ASPI advised the committee that TikTok has the ability to detect political speech, because it 'monitors key words in posts for content related to elections so that it can then attach links to its in-app election centre'. ASPI cited experiments conducted by non-profit group Accelerate Change, which found that using certain political words in TikTok videos decreased their distribution by 66 per cent. ASPI further advised that in 2020, US TikTok executives had noticed that views for certain political content creators were dropping 30 to 40 per cent. The executives later 'found out that a team in China had made changes to the algorithm to play down political conversations about the election'.¹²⁸
- 6.142 Ms Woods-Joyce of TikTok told the committee that 'TikTok is not moderated based on political sensitivities'. When asked whether TikTok had done so in the past, she conceded that 'in the past that we have not always made the correct moderation decisions' but did not specify exactly what changes had been made to ensure that did not occur again. This attempted evasion of straightforward questions, which was a consistent feature of Ms Woods-Joyce's evidence before the committee, reflected poorly on her as a witness.¹²⁹
- 6.143 However, ASPI highlighted that manipulation of content is not limited to TikTok. ASPI noted an example in February 2023, where 'Twitter chief executive Elon Musk rallied a team of roughly 80 engineers to reconfigure the platform's algorithm so his tweets would be more widely viewed'. ASPI advised that there is 'clearly a need for all social media companies to be more transparent about how changes to their algorithms affect the content users receive'.¹³⁰

Evading oversight

- 6.144 Commissioner Carr also raised concerns with the manner in which TikTok engages with regulation and oversight:

When a senior TikTok official—I believe the COO [Chief Operating Officer]—was testifying here in our Senate a few months ago they were asked point-blank, 'Do you share sensitive US user data with personnel—TikTok or ByteDance—in Beijing that are themselves members of the CCP?' That official declined to answer that question. I think a lot of these concerns could have been put to rest if they had answered pointedly and either said

¹²⁷ Australian Strategic Policy Institute, *Submission 13*, p. 9.

¹²⁸ Mr Fergus Ryan, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 19

¹²⁹ Ms Ella Woods-Joyce, TikTok, *Committee Hansard*, 11 July 2023, pp. 29–30.

¹³⁰ Australian Strategic Policy Institute, *Submission 13*, p. 10.

no or, frankly, perhaps said, 'Yes, and here are the protections put in place.'
The evasive nature of these answers over years is deeply concerning.¹³¹

6.145 Mr David Robinson of Internet 2.0 raised similar concerns. His organisation highlighted a number of concerns with TikTok's data collection, and noted in their response that:

TikTok have never actually been transparent. TikTok have never said, 'Internet 2.0 is wrong because of this piece of code and it actually does this and this,' and printed lines of their code in a transparent way. They've always just called us names and spent a lot of money on anti campaigns. From my perspective, every other social media company that we engage with has come back and qualified their position. Companies like Proton and Telegram, when asked, qualified their position and explained exactly what their things do. TikTok have never done this with evidence.¹³²

6.146 Mr Robinson compared the TikTok response to Proton, saying that Proton 'just sent us the GitHub, and we analysed that and it came out exactly the same because it's a transparent way to do things' and further noted in relation to TikTok's response that 'when people deny stuff, normally you've found their sensitive spot'.¹³³

6.147 This evasive nature was evident in the manner in which TikTok's Australian executives responded to questions posed by the committee at a public hearing on 11 July 2023. When asked a simple question, Ms Woods-Joyce avoided agreeing with the premise that ByteDance is a Chinese company, despite the submission stating TikTok is proud of 'our company's Chinese heritage'. Further, Ms Woods-Joyce avoided answering whether Bytedance is headquartered in China, stating that 'ByteDance has operations around the world', later conceding the existence of 'offices in China'.¹³⁴

6.148 These answers are consistent with news reports that leaked 'internal documents show TikTok is actively instructing employees to "downplay the China association" to deflect growing media scrutiny over the video-sharing app's Beijing-based owner'.¹³⁵

¹³¹ Mr Brendan Carr, Commissioner, United States Federal Communications Commission, *Committee Hansard*, 20 April 2023, p. 7.

¹³² Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 31.

¹³³ Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 32.

¹³⁴ Ms Ella Woods-Joyce, TikTok, *Committee Hansard*, 11 July 2023, p. 21; TikTok, *Submission 30*, p. 2.

¹³⁵ Thomas Barrabi, ['Leaked TikTok memo told employees to downplay the China association'](#), *NY Post*, 27 July 2022.

6.149 This is further highlighted by the March 2023, resignation of a senior ByteDance executive from the Australian board of TikTok, amid the viral video platform's efforts to distance itself from its Chinese parent company.¹³⁶

Data safety

6.150 This issue of data collection by the CCP has been one of increasing concern to the global intelligence community. Mr Richard Moore, head of the UK's intelligence agency, MI6, recently warned that:

China has added to its immense datasets at home by hoovering up others abroad, and the Chinese authorities are not hugely troubled by questions of personal privacy, or individual data security. They're focused on controlling information and preventing inconvenient truths from being revealed.¹³⁷

6.151 Ms Yaqiu Wang of Human Rights Watch noted that all social media platforms gather data, but while most do so for the purposes of 'selling you more things', Chinese-based companies were subject to the control of the CCP, which 'has political goals beyond profits'.¹³⁸

6.152 Internet 2.0 argued for actions to keep data safe from authoritarian regimes:

As social media companies are the primary producer of high quality social, psychological, political, military, and economic data, liberal democracies must move to defend this data by limiting the access to it by authoritarian regimes.¹³⁹

6.153 The approach of data localisation, where user data is housed in databanks outside of mainland China, is currently being considered by platforms in the European Union (EU; Project Clover) and the US (Project Texas). Details were outlined in Chapter 3. Experts advised this committee that a similar approach could be taken here, but qualified that it would not be a 'silver bullet' solution.

6.154 Mr David Robinson of Internet 2.0 noted that while a single mechanism would not work, he believed that 'some form of local data storage is required' because 'we lose the ability to control how that data is regulated once it leaves our shores'. Mr Robinson further explained the difficulties in regulating offshore data:

... the Australian Privacy Act is limited to Australian waters, basically. As soon as that data leaves Australia, it's up to you to have an alliance or an

¹³⁶ Max Mason, ['ByteDance executive resigns from TikTok Australia board'](#), *Australian Financial Review*, 21 March 2023.

¹³⁷ Alexander Martin, ['Head of MI6 warns that China is setting "data traps" for partners'](#), *The Record*, 19 July 2023.

¹³⁸ Ms Yaqiu Wang, Human Rights Watch, *Committee Hansard*, 21 April 2023, p. 6.

¹³⁹ Internet 2.0, *Submission 17*, p. 5.

agreement with the other country that your law still applies. If you sell the data to China and it's in China, Chinese law applies.¹⁴⁰

6.155 Mr Robinson noted the difficulties this presents during an election, where if data is sitting in a country that doesn't cooperate with Australia, the ability to have it taken down quickly is reduced and the statements have longer to have an impact. If data is sitting in Australia or the US, it can likely be taken down within hours.¹⁴¹

6.156 Mr Robinson further advised that Australia should look to data collection laws in the EU:

... the GDPR [General Data Protection Regulation] is probably a better system of regulating how data is used. The ability of Western social media companies to collect and sell users' data in Europe is far less than in Australia and the US—so I can't buy sophisticated advertising data easily in European jurisdictions as I can in Australia and the US, because of the way the act works.¹⁴²

6.157 Ms Shanthi Kalathil noted that data collection is not only occurring via social media platforms. She advised that Chinese participation in smart city platforms in a number of countries also provided an opportunity for data collection, and in particular the gaming sector is a place where significant amounts of data can be collected, but that sector 'frequently does not get included in the kinds of conversations that we're having here today'.¹⁴³

6.158 Ms Kalathil agreed that data localisation may help to mitigate the risk, but noted that 'you can't use primarily a technical or legal solution to what ultimately is a political problem'.¹⁴⁴

6.159 Commissioner Carr concurred that data localisation [Project Texas in the US] would not provide sufficient protections, and cited a relevant news article:

The BuzzFeed news article got leaked internal audio from TikTok DC [District of Columbia] officials saying that, even after Project Texas was put in place, 'It remains to be seen if product and engineering'—meaning Beijing—'would continue to have access to the data.' If TikTok officials themselves don't believe that Project Texas is actually going to safeguard data against access from inside China, I think we should take their word for it.¹⁴⁵

¹⁴⁰ Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 34.

¹⁴¹ Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 35.

¹⁴² Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 35.

¹⁴³ Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, p. 4.

¹⁴⁴ Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, p. 4.

¹⁴⁵ Mr Brendan Carr, United States Federal Communications Commission, *Committee Hansard*, 20 April 2023, p. 8.

6.160 Commissioner Carr recommended the best approach would be a ban or genuine divestiture, for example where ByteDance would be forced to sell TikTok to a non-Chinese, mainland US company.¹⁴⁶

6.161 ASPI also expressed doubt at the usefulness of data localisation:

TikTok will always say that TikTok user data is stored in Singapore or in the United States. That is really immaterial if that data continues to be accessed from Beijing.¹⁴⁷

Impact on Chinese-language media

6.162 A key concern of experts was the chilling effect that WeChat can have on independent Chinese-language media. Dr Kaplan noted that these independent media outlets 'because of advertising and WeChat and possibly because they want to do business in China, are self-censoring completely'.¹⁴⁸

6.163 Human Rights Watch raised similar concerns that local Chinese-language media self-censors so their content will be allowed on WeChat:

Then, as a local news website operator, because your account is on WeChat, you have to think about what can be published on WeChat. So you self-censor ... A diaspora outlet that caters to the diaspora has to go through Beijing's censors. Even what's going on in Australia is censored by Beijing. That's the news side.¹⁴⁹

6.164 Dr Kaplan, informed the committee that it is not just federal issues of concern, but that in the US 'the state level may be more vulnerable than the federal level'. Dr Kaplan noted that 'WeChat is managing information, helping to mobilise Chinese speakers and then seeking coalition partners among the non-Chinese-language-speaking civil society, and all this, basically, is direct interference in the politics of the country'.¹⁵⁰

TikTok bans

6.165 On 17 March 2022, New Zealand's Parliamentary Service announced it was blocking TikTok from all parliamentary devices. This followed a ban in November 2022 preventing members of New Zealand's Defence Force from having the app on government issued phones, joining the Ministry of Education, Ministry of Foreign Affairs and Trade, Department of Prime Minister and

¹⁴⁶ Mr Brendan Carr, United States Federal Communications Commission, *Committee Hansard*, 20 April 2023, p. 8.

¹⁴⁷ Mr Fergus Ryan, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 22.

¹⁴⁸ Dr Seth Kaplan, *Committee Hansard*, 20 April 2023, pp. 12 and 17.

¹⁴⁹ Ms Yaqiu Wang, Human Rights Watch, *Committee Hansard*, 21 April 2023, p. 4.

¹⁵⁰ Dr Seth Kaplan, *Committee Hansard*, 20 April 2023, p. 12.

Cabinet, Corrections, Police, Treasury, Ministry of Justice, and Ministry of Primary Industries.¹⁵¹

6.166 Canada's Federal Government banned TikTok on government-issued devices in February 2023.¹⁵²

6.167 When questioned on the decisions to ban TikTok and security concerns raised by the governments of the US, Canada, France, the UK, the European Commission, New Zealand and Denmark Ms Woods-Joyce of TikTok said 'we don't believe there's any evidence to support the view that TikTok is in any way a national security threat, as might be implied by some of the commentary about us'.¹⁵³

6.168 However, when the same question was immediately posed to Mr Will Farrell, a TikTok US Security Officer, he gave an opposite response and said 'we've never pushed back on the concerns' and then clarified that meant 'we choose not to argue about the concerns'.¹⁵⁴ Mr Farrell was portrayed to the committee as a technical expert who could answer questions about the operation of the app, but was frequently not able to do so. TikTok's decision to make available witnesses to the committee who were not able to assist with obvious questions indicates they did not intend to genuinely engage in the committee process.

6.169 The Australian Signals Directorate provided an extensive outline to the committee on the nature of the advice it gave the Australian Government; advice which was a considerable factor in the decision to ban the app from government-issues devices:

ASD's [Australian Signal Directorate's] technical advice centres on its analysis of the business model which is employed by TikTok which, like other social media platforms, operates on the basis of collecting user information. That information and data collection includes data, user generated content and device data. The application can also identify other applications in use on the device and any browsing activity undertaken within the TikTok web browser. The other data may include users' names, email addresses, phone numbers, contacts, photos, user IDs [identifications], ad [advertising] identifiers and data stored in the device clipboard while TikTok is in use. Device data may include SIM card and IMSI [international mobile subscriber identity] numbers, device type and model, language, time zone, unique device IDs, running of installed apps, IP [internet protocol]

¹⁵¹ Tess McClure, '[New Zealand to ban TikTok from government devices](#)', *The Guardian*, 17 March 2023; Thomas Manch, '[Defence Force orders TikTok to be wiped from phones, as government agencies grapple with data risks](#)', *Stuff*, 4 March 2023.

¹⁵² Alex Hern, *the Guardian*, '[Canada bans TikTok on government devices over security risks](#)', 1 March 2023.

¹⁵³ Ms Ella Woods-Joyce, TikTok, *Committee Hansard*, 11 July 2023, p. 30.

¹⁵⁴ Mr Will Farrell, Security Officer, TikTok US Data Security Inc, *Committee Hansard*, 11 July 2023, pp. 30–31.

addresses, telecommunication provider details and details of the devices on the same network.

...

Finally—and not so much technical but associated with the technical risks—is the risk of foreign ownership. I heard the committee comment before on the operation of the Chinese national intelligence law which requires that citizens, companies and organisations cooperate, and there is capacity to ask for that cooperation not to be disclosed.¹⁵⁵

6.170 Several Australian Government departments have also implemented restrictions on WeChat, including the Department of the Prime Minister and Cabinet, the Department of Foreign Affairs and Trade, and Home Affairs.¹⁵⁶

Bans or divestment

6.171 There was disagreement among expert witnesses as to whether the best security mitigation for platforms that originate from authoritarian states was usage bans, standards-based regulation or divestment of platforms to companies that would be wholly subject to local laws.

6.172 Dr Seth Kaplan argued against an outright ban on WeChat because it would be too difficult to implement. Dr Kaplan instead pointed to setting standards via regulation, but noted that it would be difficult for WeChat to meet those standards 'given the way China operates and the way Tencent is related to the government'. Dr Kaplan further noted that WeChat could not be divested in the same way that TikTok could be.¹⁵⁷

6.173 ASPI did not go so far as to call for a ban of such platforms and applications, but recommended 'bespoke legislation that deals with TikTok and any other emerging major social media apps from authoritarian countries'.¹⁵⁸

6.174 Mr David Robinson of Internet 2.0 argued against banning specific apps because companies could quickly use the source code to make a new app and argued that applying 'legislation and regulation to the software and the code and how it acts is more important than the specific company'.¹⁵⁹

¹⁵⁵ Ms Abigail Bradshaw, Australian Signals Directorate, *Committee Hansard*, 12 July 2023, p. 3.

¹⁵⁶ Gus McCubbing, ['Banning WeChat would 'damage' democracy, experts say'](#), *Australian Financial Review*, 4 May 2023; Josh Taylor, ['Australian government resists blanket WeChat ban despite restrictions by multiple departments'](#), *The Guardian*, 28 April 2023.

¹⁵⁷ Dr Seth Kaplan, Private capacity, *Committee Hansard*, 20 April 2023, pp. 13–14.

¹⁵⁸ Mr Fergus Ryan, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 19.

¹⁵⁹ Mr David Robinson, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 33.

6.175 Ms Yaqui Wang of Human Rights Watch also argued in favour of standards-setting legislation, which included shutdown clauses for non-compliance.¹⁶⁰

6.176 Ms Lindsay Gorman of the Alliance for Securing Democracy argued for forced divestiture of TikTok, given its large user base and incorporation into the wider information environment:

That makes it very, very difficult to contemplate something like a ban. That is why it's my view that a forced divestiture, whereby the concerns could be partially mitigated by the removal of TikTok's Chinese ownership by ByteDance, would allow TikTok to keep operating in democracies without that overwhelming threat of foreign influence and interference.¹⁶¹

6.177 However, Ms Gorman stressed that this approach should be taken in conjunction with establishing legislated safety frameworks for future apps and platforms 'so that we can get ahead of these threats before they become one of the most popular apps in the country and in the world, and we can address them head-on before getting into the scenario that is not a great one that we find ourselves in today'.¹⁶²

6.178 Mr Kenny Chiu, a Canadian MP who was subjected to foreign interference during an election, argued against 'just abruptly banning WeChat from all usage, because the shock that could go around the community and the diaspora would be huge and could sever many ties that they have, be they business ties or, even worse, familial ties with family members'. He advised that western liberal democracies should instead try to 'encourage our citizens, through education and persuasion, to diversify and not rely on one single app'.¹⁶³

6.179 The artist Badiuca argued in favour of standards-based regulation that would, at its essence, protect free speech:

I do believe Australians should have regulation to make companies like WeChat follow our laws, respect our way of life and value our freedom of speech. If they fail to obey those regulations then punishment or even banning should be a possible option in order to protect the rights of the people who are living in Australia. This has nothing to do with racism or xenophobia. This is actually to defend universal human rights. This is also how the Chinese diaspora can benefit from this mechanism because now we don't need to be subject to the Chinese government's tyranny and control. Regardless of whether you're using Chinese, English, Mandarin or Cantonese, with any platform we shall have the right to express ourselves

¹⁶⁰ Ms Yaqui Wang, Human Rights Watch, *Committee Hansard*, 21 April 2023, p. 3.

¹⁶¹ Ms Lindsay Gorman, Alliance for Securing Democracy, *Committee Hansard*, 21 April 2023, p. 9.

¹⁶² Ms Lindsay Gorman, Alliance for Securing Democracy, *Committee Hansard*, 21 April 2023, p. 9.

¹⁶³ Mr Kenny Chiu, Private capacity, *Committee Hansard*, 21 April 2023, p. 18.

instead of being censored, controlled and intimidated by this foreign government in China.¹⁶⁴

¹⁶⁴ Badiucao, *Private capacity*, *Committee Hansard*, 21 April 2023, p. 35.

Chapter 7

Building the capacity of civil society

- 7.1 Crucial to a comprehensive and coordinated approach to countering foreign interference through social media is inclusion of, and collaboration with, civil society. A common recommendation across many submissions was the need to improve the capacity and resilience of both individuals and civil society to respond to disinformation, degradation of public trust in democratic institutions, and foreign interference through social media.¹
- 7.2 In addition to government and platform-based solutions discussed in Chapters 4 to 6 this chapter discusses the role for non-government institutions and civil society to address foreign interference through social media.
- 7.3 Initiatives to build capacity and resilience in civil society should at times be supported and/or funded by government, with the groundwork primarily undertaken by non-government bodies, specifically through:
- independent fact checking, expert centre monitoring, research and solutions development;
 - civil litigation;
 - building resilience in communities through public and school education;
 - impartial and independent reporting through mainstream media; and
 - improving knowledge, capacity and community cohesion in diaspora and culturally and linguistically diverse (CALD) communities.
- 7.4 Nevertheless, Reset Australia warned against overly relying on social media end-user empowerment, arguing for a more comprehensive government and platform response to foreign interference through social media rather than shifting the burden to citizens and communities.²

A role for civil society organisations, expert centres and researchers

- 7.5 Fact checkers are engaged directly by social media platforms to mitigate against disinformation, as discussed in Chapter 6. However, beyond these, other civil society-based researchers provide additional independent commentary and scrutiny to help inform and highlight disinformation and foreign influence.

¹ See, for example: Information and Influence University Partnership (comprising University of Adelaide, University of Melbourne and University of New South Wales), *Submission 28*, p. [3]; Meta, *Submission 32*, p. 18; Department of Home Affairs, *Submission 1*, pp. 4–5; Australian Security Intelligence Organisation, *Submission 2*, p. 7; Australian Human Rights Commission *Submission 9*, p. 9; News and Media Research Centre, University of Canberra, *Submission 21*, pp. 4–5.

² Reset Australia, *Submission 26*, pp. 2 and 7–8. See also: CyberCX, *Submission 16*, pp. 9–10.

- 7.6 This unique role played by independent civil society organisations (such as fact checkers and expert centres) and researchers was highlighted by submitters to the inquiry, with Reset Australia calling these bodies 'the canaries in the coal mine sounding the alarm for emerging threats to Australian society'.³ The importance of these services was reiterated by Mr Kenny Chiu, a former Canadian politician, who recommended that:
- Australia should perhaps provide a seal of approval to certain non-government organisations that provide fact-checking services to the constituents in their own language, be it Persian, Russian or even Chinese and other languages that are commonly exploited. This would be effective in providing a way for the diaspora community to at least realise that they are being used and manipulated and that their interests are actually being hurt by these predatory regimes that are infiltrating us.⁴
- 7.7 The Defence and Security Institute within the University of Adelaide suggested that civil society expert centres (such as the Defence and Security Institute) have the ability to 'play a significant role in the development of a national capability to **detect**, **defend**, and **disrupt** social influence operations both online and offline' and contribute to the development of policy and public education responses.⁵
- 7.8 As discussed in Chapter 6, social media platforms provide some data and tools to help improve their transparency. However, as highlighted in a joint submission from University technical expert centres, 'the technical capacity to detect and analyse disinformation operations is concentrated in the hands of the platforms and a few specialised research and monitoring bodies'. The submission highlighted that although this capacity is limited it is crucially important, with the resulting information enabling civil society to 'monitor platform and government action against ongoing or real-time disinformation operations'.⁶
- 7.9 Professor Rory Cormac of the University of Nottingham noted that while he viewed fact checking as important, he advised that it has limitations—people

³ Reset Australia, *Submission 26*, p. 2; CyberCX, *Submission 16*, pp. 4 and 9, Australian Strategic Policy Institute, *Submission 13*, p. 12.

⁴ Mr Kenny Chiu, Private capacity, *Committee Hansard*, 21 April 2023, p. 16.

⁵ Emphasis in the original submission. Defence and Security Institute, *Submission 3*, pp. 3 and 7. See also: Australia Institute, *Submission 31.2: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 20.

⁶ University of New South Wales (NSW) Allens Hub for Technology Law and Innovation, Deakin University Centre for Cyber Security Research and Innovation and Institute of Electrical and Electronics Engineers (IEEE) Society on Social Implications of Technology (University Centres Joint Submission), *Submission 19*, pp. 6–7. See also: Australia Institute, *Submission 31: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 4., p. 2.

may not believe the fact checkers, particularly those 'who are inherently sceptical of the state'.⁷

- 7.10 Submitters suggested that utilisation of civil society-based expertise could be more inclusive and draw on a greater number of expert voices, work more innovatively across disciplines, potentially place more pressure on platforms and government to address disinformation and 'prevent the appearance of government and platforms acting like "Big Brother", secretively and only selectively cracking down on some disinformation while tolerating others'.⁸
- 7.11 The Information and Influence University Partnership went further, recommending the establishment of a new organisation to coordinate monitoring and operational responses to malicious information threats, drawing on a pool of expert, multidisciplinary academic and industry partners.⁹
- 7.12 However, several witnesses highlighted that access to platforms' data (in a way that preserves privacy) can be challenging.¹⁰ Mr Josh Machin from Meta explained that:

... many folks within the industry are broadly supportive of transparency and working with academics, but there can be very challenging considerations to work around, particularly from a privacy perspective ... it's an area in which we continue to work very hard and make more information available to support academics, experts and policy makers in scrutinising content on our services.¹¹

- 7.13 Submitters and witnesses also advised that adequate funding is essential to enable civil society organisations, independent researchers and expert centres to effectively fulfill this monitoring, research and solutions development role.¹²
- 7.14 While Australian Government agencies, such as the Department of Defence and the Australian Research Council, already provide some funding to expert centres to conduct relevant research, Reset Australia contended that 'they suffer from extremely limited resourcing'.¹³ CyberCX called for the Australian Government to facilitate more independent research into

⁷ Professor Rory Cormac, Director, Centre for the Study of Subversion, Unconventional Interventions and Terrorism, University of Nottingham, *Committee Hansard*, 20 April 2023, p. 40.

⁸ University Centres Joint Submission, *Submission 19*, pp. 6–7; Defence and Security Institute, University of Adelaide (Defence and Security Institute), *Submission 3*, pp. 2–3 and 7.

⁹ Information and Influence University Partnership, *Submission 28*, pp. [4–5].

¹⁰ Improved transparency and access to platform data is discussed in Chapter 6. Reset Australia, *Submission 26*, p. 2; CyberCX, *Submission 16*, p. 19.

¹¹ Mr Josh Machin, Head of Public Policy, Australia, Meta, *Committee Hansard*, 11 July 2023, p. 8.

¹² Reset Australia, *Submission 26*, p. 2; CyberCX, *Submission 16*, p. 9.

¹³ Defence and Security Institute, *Submission 3*, pp. 2–3 and Reset Australia, *Submission 26*, p. 2.

'investigating, exposing and analysing social media interference and malign influence', for example through grant funding.¹⁴

- 7.15 Social media platform Meta, likewise supported engagement with industry and civil society experts as well as technical research to improve policy and operational responses and the detection of malicious threats.¹⁵

Litigation

- 7.16 Australian Supporters of Democracy in Iran discussed the use of courts and litigation by civil society as a potential means to address disinformation campaigns and the distribution of hate material. It also noted that Australian policy and governance appears to be under-developed in this area, with civil law primarily impacting on social media 'mainly through libel and defamation cases', rather than action relating to foreign interference.¹⁶

Building resilience through public education

- 7.17 Many submitters raised the need for robust public education campaigns to counter to disinformation and foreign interference through social media, with a particular focus on improving information and media literacy, and empowering individuals to manage their online interactions.¹⁷
- 7.18 Witnesses drew attention to the wider context of rising distrust in public institutions, more polarised and extreme societal and political divisions, and an increase in conspiratorial thinking.¹⁸
- 7.19 Furthermore, the Law Council of Australia highlighted the growing market for 'disinformation-for-hire' which 'differs from genuine political campaigns because it is covert, deceptive, and manipulates public discourse to undermine democratic participation'.¹⁹

¹⁴ CyberCX, *Submission 16*, p. 9.

¹⁵ Meta, *Submission 32*, p. 17.

¹⁶ Australian Supporters of Democracy in Iran, *Submission 23*, pp. 4–5.

¹⁷ See, for example: News and Media Research Centre, University of Canberra, *Submission 21*, pp. 5 and 17; Law Council of Australia, *Submission 27*, p. 3; CyberCX, *Submission 16*, pp. 4 and 8; Australian Tibetan Community Association, *Submission 31*, p. 5; Department of Home Affairs, *Submission 1*, pp. 4–6; Australian Human Rights Commission, *Submission 9*, pp. 9–10; Information and Influence University Partnership, *Submission 28*, pp. [2–3]; RAND, *Submission 11*, p. 3; Ms Mia Garlick, Regional Director of Policy, Meta, *Committee Hansard*, 11 July 2023, p. 9.

¹⁸ See, for example: News and Media Research Centre, *Submission 21*, p. 5; CyberCX, *Submission 16*, pp. 2 and 7–8; Reset Australia, *Submission 26*, pp. 1–2; Australian Muslim Advocacy Network, *Submission 24*, p. [3]; Australian Human Rights Commission, *Submission 9*, pp. 5–7; RAND Australia, *Submission 11*, p. 2.

¹⁹ Law Council of Australia, *Submission 27*, p. 2.

- 7.20 The News and Media Research Centre of the University of Canberra called for information and media literacy measures to be considered within this bigger picture with a quotation from the North Atlantic Treaty Organization's Centre for Media Literacy:

"Democracy stands or falls on people. The challenge for democracies is to find ways to preserve the freedoms that come with more access to information, while protecting against the threats that come with it. The most democratic way to address this challenge is teaching [members of] society to be wiser information consumers and producers through critical thinking and a pedagogy that empowers them to evaluate, analyse, and choose critically whether to act on information. Media literacy education facilitates this critical thinking and thereby, risk management".²⁰

- 7.21 The Department of Home Affairs (Home Affairs) outlined its current engagement and education initiatives, including in a variety of community languages, through the Australian Values social media channels, and in partnership with other government agencies, non-government organisations and community members. The Australian Cyber Security Centre also monitors threats and provides security advice to citizens and government to ensure account holders are aware of social media risks and their social media accounts are secured.²¹
- 7.22 Social media platforms, including Meta and TikTok, have committed to promoting and investing in digital literacy education, and provide fact checkers, tools, policies and processes to help their users make informed decisions about content, to identify authentic sources of information and stay safe.²²
- 7.23 CyberCX submitted that the public is not sufficiently well-informed about the risks and responses associated with foreign interference through social media:

The information available to Australian citizens regarding foreign interference orchestrated through social media is patchy and generic, despite the key role citizens, the private sector and state and local governments play as vectors and victims of interference.

Citizens and private organisations lack the expertise, resources and access to understand the risks of every social media platform they engage with. This problem is exacerbated by the opacity and complexity of platforms' software and terms of service and, in some cases, links with authoritarian governments.²³

²⁰ News and Media Research Centre, *Submission 21*, pp. 4 and 5.

²¹ Department of Home Affairs, *Submission 1*, pp. 4–6; Department of Home Affairs, answers to questions on notice (no. 7), 12 July 2023 (received 18 July 2023).

²² TikTok, *Submission 30*, pp. 1, 4–5 and 10; Meta Australia, *Submission 32*, pp. 14–16 and 18; Digital Industry Group Inc., *Submission 36*, p. 2.

²³ CyberCX, *Submission 16*, p. 8.

7.24 Public education campaign models used overseas, as discussed in Chapter 2, could provide models for similar Australian campaigns. Submitters to the inquiry recommended a range of public education approaches to 'improve digital literacy and awareness, as well as to build resilience to misinformation and disinformation' and foreign interference through social media,²⁴ including:

- increased visibility or exposure of the scale of foreign interference in Australia;²⁵
- more comprehensive and 'actionable, specific advice' regarding individual platforms;²⁶
- how communities and individuals can report instances of foreign interference through social media, including through workshops;²⁷
- education and guidance materials on values, critical thinking, how users can identify and counter misinformation and disinformation, how algorithms use personal data to tailor online experiences and how users can protect themselves on social media;²⁸ and
- accessible and tailored education materials to meet the needs of all Australians, including across age demographics and CALD communities.²⁹

7.25 Mr Albert Zhang of ASPI highlighted the role that government has in providing information to support civil society through public education:

The key takeaway and what the government could do is to actually be more transparent and offer more information where individuals, society or businesses can't do the research or do the due diligence to verify the information itself. This is really pertinent when it comes to foreign based or state backed disinformation or foreign interference. The individual is not going to be able to detect whether an authoritarian security agency is running an influence campaign against them. So, in those cases, it's really

²⁴ Law Council of Australia, *Submission 27*, p. 3; Information and Influence University Partnership, *Submission 28*, pp. [2–3]; Australian Strategic Policy Institute, *Submission 13*, pp. 14–15.

²⁵ Law Council of Australia, *Submission 27*, p. 3.

²⁶ CyberCX, *Submission 16*, pp. 7–8; Ms Vicky Xu, Senior Fellow, Australian Strategic Policy Institute, *Committee Hansard*, 21 April 2023, pp. 35–36.

²⁷ Mr Kalsang Tsering, President, Australian Tibetan Community Association, *Committee Hansard*, 21 April 2023, p. 26.

²⁸ CyberCX, *Submission 16*, pp. 7–8; Australian Tibetan Community Association, *Submission 31*, p. 5; Australian Human Rights Commission, *Submission 9*, pp. 9–10 and 12; University Centres Joint Submission, *Submission 19*, Attachment 1, p. [4].

²⁹ Australian Human Rights Commission, *Submission 9*, p. 10; eSafety Commissioner, *Submission 10*, p. [2]; Cyber CX, *Submission 16*, p. 4.

important for government to disclose their intelligence or disclose their findings to the public who are being targeted.³⁰

- 7.26 The News and Media Research Centre suggested better engagement with media professionals and associations, peak professional bodies and community sector groups with expertise in media and information literacy training and in the provision of public education programs and resources. The centre further recommended funded research into the impacts of new media technology and how best to deliver media and information literacy.³¹
- 7.27 At the April 2023 public hearing, Dr Andrew Dowse from RAND Australia drew attention to a training package it is developing for a government client 'to help people identify, understand and protect themselves from foreign interference ... efforts to increase media literacy are critical in relation to that challenge, but they are not the only solution'.³²
- 7.28 Similarly, Mr Richard Salgado, Director, Law Enforcement and Information Security, Google, noted that such government-run campaigns are not a panacea for the problem of foreign interference and disinformation on social media. Mr Salgado stated that:

I would say my experience with this and what we have seen so far would suggest that there is probably no single voice that's going to be effective; it has to be a chorus of voices. There are going to be plenty of people who are not going to believe a government agency when they say it, just as there would be plenty who won't believe it if a company or security researchers were to say it. I don't think that there is an answer in the terms of a single voice that will be heard by all those who you want the message to get to.³³

Electoral public education

- 7.29 There has not been any identified foreign interference compromising the integrity of the 2022 Australian federal election. However, there are alleged examples of foreign interference in other democratic countries, most notably Russian interference in the 2016 United States' Presidential election and 2022 midterm elections.³⁴ As noted by Internet 2.0:

³⁰ Mr Albert Zhang, Analyst, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 24.

³¹ News and Media Research Centre, *Submission 21*, p. 17.

³² Dr Andrew Dowse, Director, RAND Australia, *Committee Hansard*, 20 April 2023, pp. 27 and 30.

³³ Mr Richard Salgado, Director, Law Enforcement and Information Security, Google, *Committee Hansard: Foreign Interference through Social Media inquiry (46th Parliament)*, 30 July 2021, p. 13.

³⁴ Australian Electoral Commission, *Submission 8*, p. 2; RAND Australia, *Submission 11*, pp. 2–3; Australian Strategic Policy Institute, *Submission 13*, pp. 2 and 4; Dr William Stolz, Senior Fellow, National Security College, Australian National University, *Submission 18*, pp. 15–16; Reset Australia, *Submission 26*, pp. 5–6; Rachel Lee, Prudence Luttrell, Matthew Johnson and John

... elections are a strategic opportunity to influence our democratic process. They [Australia's authoritarian competitors] believe that it is to their benefit if the voting population have less confidence in the true results of elections. By conducting divisive campaigns, they seek to divide our societies, to weaken us, and to fracture our uniting values.³⁵

- 7.30 The Information and Influence University Partnership further explained the dangers of foreign interference in electoral processes, including through social media:

Foreign interference can thwart democratic participation in nation-building. ... Disinformation operations can be used broadly to normalise anti-democratic views and actions, microtargeted to cultivate extremist views, and even to radicalise some segments of the population. Such operations may recruit and incite radicalised individuals and groups to engage in anti-democratic activities and assaults on the institution of democracy itself. Moreover, public displays of anti-democratic behaviours (and foreign operations to fuel them) may undermine the legitimacy of democracy as an institution, erode the citizens' trust in the apparatus of democracy—parliament, government, and judiciary—and cause disillusionment, disenchantment, and apathy, thereby threatening democratic participation.³⁶

- 7.31 As such, public education in relation to electoral matters was a specific area of interest raised by several witnesses. The Australian Electoral Commission (AEC) highlighted that:

Determining the success of any parliamentary election is ensuring that not only is every ballot counted, re-counted and results certified, but that Australians have confidence in the outcome.³⁷

- 7.32 The AEC noted that Australia's laws regulate electoral and political communications, however they do not, in general, regulate truth in electoral advertising:

... with one limited exception, it does not regulate truth in electoral communication. Furthermore, the High Court has found there is an implied freedom of political communication in the Commonwealth Constitution that limits the scope of the Parliament to make laws restricting political communications.³⁸

Garnaut, *Submission 34*, pp. 4–5; Professor Rory Cormac, University of Nottingham, *Committee Hansard*, 20 April 2023, p. 38.

³⁵ Internet 2.0, *Submission 17*, p. 6.

³⁶ Information and Influence University Partnership, *Submission 28*, p. [2].

³⁷ Australian Electoral Commission, *Submission 8*, p. 1. See also CyberCX, *Submission 16*, p. 2.

³⁸ Australian Electoral Commission, *Submission 8*, p. 2. See also Ms Sally Pfeiffer, Acting First Assistant Secretary, Counter Foreign Interference, Department of Home Affairs, *Committee Hansard*, 12 July 2023, pp. 8–9.

7.33 Nevertheless, a survey conducted by the AEC found that 80 per cent of those surveyed:

... believed the Australian Government has a responsibility to educate people about disinformation on social media. In addition, 48 per cent of those surveyed reported seeing false or misleading content on social media (an increase from 38 per cent at benchmark) and 67 per cent agreed that groups/individuals deliberately spread false information online about voting.³⁹

7.34 Witnesses drew attention to preparations for the 2022 federal election and the range of measures adopted by the AEC. These included a nationwide education and advertising campaign, establishing a disinformation register, working with platforms, including the development of a *Statement of Intent for the Federal Election 2022*, referring disinformation to online platforms for review and responding directly to disinformation online (for example through Twitter).⁴⁰

7.35 In March 2023, it was reported that the AEC 'is looking to go a step further and set up information sharing arrangements with Australian Associated Press (AAP) Fact Check, RMIT FactLab and RMIT ABC Fact Check' in the lead up to the upcoming referendum on an Indigenous Voice to Parliament.⁴¹

7.36 Platforms also have a role in 'the promotion of authoritative sources of information, partnering with fact checking organisations, and collaborating with the Australian Electoral Commission' to address election-related disinformation and to promote authoritative AEC content, including in the lead up to The Voice referendum.⁴²

7.37 TikTok drew attention to its election-related measures, including its work with partners such as AAP FactCheck, as well as prohibitions on political advertising, which in 2023 are being extended to restrict solicitations for campaign funding and political party donations.⁴³ It also highlighted its in-app election guide which 'provided detailed, authoritative information on the election process,

³⁹ Australian Electoral Commission, *Submission 8*, p. 3.

⁴⁰ Department of Home Affairs, *Submission 1*, p. 4. See also the Australian Human Rights Commission, *Submission 9*, p. 12; Australian Strategic Policy Institute, *Submission 13*, p. 9; Digital Industry Group Inc., *Submission 35*, pp. 4–5.

⁴¹ Sam Buckingham-Jones and Mark Di Stefano, '[AEC eyes tie-up with fact-checkers for Voice referendum](#)', *Australian Financial Review*, 19 March 2023.

⁴² Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Submission 7*, p. 2. See also DIGI, *Submission 35*, p. 5; Ms Mia Garlick, Regional Director of Policy, Meta, *Committee Hansard*, 11 July 2023, p. 2.

⁴³ TikTok, *Submission 30*, pp. 5 and 6.

including information on where and how to vote and preferential voting explainers developed by the Commission [AEC]'.⁴⁴

Australian Electoral Commission's 'Stop and Consider' campaign

7.38 For the 2022 federal election, the AEC established a strong digital presence and expanded on its 2019 'Stop and Consider' public education campaign, aimed at 'encouraging voters to stop, check and consider the source of electoral information they are consuming'.⁴⁵

7.39 The AEC also placed advertising and other media placements across social media platforms, digital displays and search term advertising, as well as information in over 20 languages.⁴⁶

7.40 The AEC observed that its approach was successful, and that its:

... digital presence [was] widely recognised as one of the most forthright and informative from a government agency. Delivering on the reputation management principles, the AEC took an approach focusing on being human in tone, swift and regular in reply, and knowledgeable. This approach helped solidify our digital presence as the authoritative voice on electoral processes, providing a defence to Australian democracy from the threat of disinformation.⁴⁷

7.41 The AEC attributed the campaign's success to the fact it directly addressed disinformation online and its friendly, often humorous approach which engaged the public. Even the Washington Post reported on the campaign—quoting political scientist Ariadne Vromen—'their meme game is pretty strong ... and the informal language is really important. It's personalized. It's using everyday norms of engagement. And that is the kind of thing that people will notice and will share'.⁴⁸

7.42 The AEC's very deliberate approach to inform and engage the public and encourage reporting of disinformation resulted in numerous social media users

⁴⁴ TikTok, *Submission 30*, p. 6.

⁴⁵ Australian Electoral Commission, *Submission 8*, p. 3.

⁴⁶ Australian Electoral Commission, *Submission 8*, p. 4; Mr Tom Rogers, Electoral Commissioner, Australian Electoral Commission, *Committee Hansard*, 12 July 2023, p. 36.

⁴⁷ Australian Electoral Commission, *Submission 8*, p. 3.

⁴⁸ Michael E Miller and Frances Vinall, ['The Twitter account defending Australian democracy'](#), *The Washington Post*, 14 May 2022. See also: Cait Kelly, ["'Firm but friendly": how the AEC Twitter account is winning friends and influencing people'](#), *The Guardian*, 11 February 2022; Michelle Elias, ["'Leave the eggplant off": How the AEC is engaging online to counter fake claims about voting'](#), *SBS News*, 16 March 2022.

reporting and tagging misleading content, opening the door to the AEC stepping in with correct information.⁴⁹

- 7.43 In their submission the Law Society of New South Wales Young Lawyers recommended that the Electoral Integrity Assurance Taskforce be obliged to produce a periodic report on foreign interference through social media in Australian elections, stating that 'such a report would support vigilance among the Australian public as to what potential threats they may encounter online in upcoming elections'.⁵⁰

School-based education

- 7.44 Regarding media literacy, the Joint Standing Committee on Electoral Matters (Electoral committee) previously recommended in its *Report on the conduct of the 2016 federal election and matters related thereto* that:

... increased social media literacy, as part of a strengthened civics and electoral education curriculum, is a vital component in facing the challenges posed by this new social media environment. Australians must be better equipped to critically discern and judge any media which seeks to influence their voting behaviour.⁵¹

- 7.45 The Electoral committee subsequently recommended that:

Recommendation 30 | ... the Australian Government consider ways in which media literacy can be enhanced through education programs that teach students not only how to create media, but also how to critically analyse it.

Recommendation 31 | ... the Australian Electoral Commission examine ways in which media literacy can be incorporated into a modern, relevant civics education program.⁵²

- 7.46 A number of submitters to this inquiry highlighted the importance of school-based information and media literacy campaigns to address disinformation and foreign interference through social media.
- 7.47 Ms Emily Moseley from ASPI highlighted the effectiveness of social media disinformation education in schools in northern Europe, stating that 'in particular, younger generations that are more influenced by social media are

⁴⁹ Australian Electoral Commission, [Disinformation register: 2022 Federal Election](#), 10 January 2023 (accessed 21 July 2023).

⁵⁰ Law Society of New South Wales Young Lawyers, *Submission 33*, p. 8.

⁵¹ Joint Standing Committee on Electoral Matters, [Report on the conduct of the 2016 federal election and matters related thereto](#), November 2018, p. 61.

⁵² Joint Standing Committee on Electoral Matters, *Report on the conduct of the 2016 federal election and matters related thereto*, November 2018, pp. xxviii-xxix.

coming up in the generation and learning and determining which news sources are relevant or what to look for in terms of combatting disinformation'.⁵³

- 7.48 Home Affairs noted that in 2022–23 the Australian Government provided \$6 million funding over three years to the Alannah and Madeline Foundation to:

... develop and deliver digital and media literacy education products for primary and secondary school students. These products will be made freely available to every Australian primary and secondary school, improving digital literacy and helping students to be critical, responsible and active citizens online.⁵⁴

- 7.49 In 2022, the Australian Capital Territory Education Directorate also funded News and Media Research Centre to co-create primary school educational resources, successfully demonstrating the value of civic online reasoning education.⁵⁵
- 7.50 However, the News and Media Research Centre of the University of Canberra suggested that the current information literacy education model has failed given the wide variations between state and territory institutional responses and the teaching strategies used are commonly 'outmoded' and 'ineffectual'.⁵⁶
- 7.51 Submitters, including University technical expert centres and the Australian Human Rights Commission (AHRC), recommended curriculum changes to ensure that information and media literacy is included in Australian schools and adapted to the current environment.⁵⁷ The News and Media Research Centre further recommended appropriate education and development programs for teachers to equip them with the required knowledge and skills.⁵⁸
- 7.52 In discussing what content could be included in a school setting, Principle Co proposed teaching critical thinking and media literacy skills to students, which would allow them to 'sceptically question what [they] see and read to develop informed opinions from an early age', as well as examining the impacts of

⁵³ Ms Emily Mosley, International Cyber Policy Centre Coordinator, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 24.

⁵⁴ Department of Home Affairs, *Submission 1*, p. 6.

⁵⁵ News and Media Research Centre, *Submission 21*, p. 9.

⁵⁶ News and Media Research Centre, *Submission 21*, p. 6.

⁵⁷ University Centres Joint Submission, *Submission 19*, pp. 2–3, 6 and 16 and Attachment 1, p. [1]; Australian Human Rights Commission, *Submission 90: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 10.

⁵⁸ News and Media Research Centre, *Submission 21*, p. 16.

psychological processes such as cognitive miserliness, cognitive dissonance, confirmation bias, motivated reasoning, and repetition error.⁵⁹

Mainstream media

- 7.53 Witnesses recognised that public broadcasters and mainstream media also have public education responsibilities to provide reliable, accurate and apolitical information about current events and political matters, with ASPI arguing that this information forms 'critical infrastructure' for informed decision-making.⁶⁰
- 7.54 Discussing the declining trust in institutions, the News and Media Research Centre noted 'when people think the mainstream media is not holding industries and governments to account, they view it as a mouthpiece for elite interests, and may be more likely to accept information that challenges conventional beliefs'.⁶¹
- 7.55 Social media is increasingly the source of news content for many Australians. Dr Seth Kaplan, a US political expert, told the committee 'there are significant numbers of people using it [social media] for news and for information and are being exposed to that. I think that has great implications for your social cohesion and the trust of your government in those vulnerable communities'. Dr Kaplan further argued that for foreign language speakers the news they consume is based on a single dominant view.⁶²
- 7.56 This view was reiterated by Mr Kenny Chiu, a former Canadian MP:
- I believe that in the multicultural society that we live in, respecting everybody's rights for the flow of information, unfortunately some of the diaspora community members are living in relative information isolation, and therefore that presents a huge opportunity for these regimes such as the CCP [Chinese Communist Party] to exploit and spread disinformation among them ... they don't know what they don't know, and they have no way of fact-checking in their comfortable and preferred language.⁶³
- 7.57 In order to address the risks posed to Australia's democracy by foreign interference through social media, Human Rights Watch made a range of recommendations including promoting independent and professional journalism (in Chinese), investing in training and similar programs, and

⁵⁹ Principle Co, *Submission 25: Foreign Interference through Social Media inquiry* (46th Parliament), p. 8.

⁶⁰ Australian Strategic Policy Institute, *Submission 13*, p. 7. See, for example: Department of Home Affairs, *Submission 1*, p. 5; Special Broadcasting Service, *Submission 14*, pp. 1–4.

⁶¹ News and Media Research Centre, *Submission 21*, p. 5. See also: Australian Muslim Advocacy Network, *Submission 24*, p. [4].

⁶² Dr Seth Kaplan, Private capacity, *Committee Hansard*, 20 April 2023, p. 15. See also: Sora Park, Caroline Fisher, Kieran McGuinness, Jee Young Lee, and, Kerry McCallum, *Digital news report: Australia 2021*, June 2021, p. 10; Badiucuo, Private capacity, *Committee Hansard*, 21 April 2023, p. 37.

⁶³ Mr Kenny Chiu, Private capacity, *Committee Hansard*, 21 April 2023, p. 16.

investing in other open-source technologies to provide other channels of communication to enable communities to more easily bypass censorship.⁶⁴

- 7.58 Principle Co similarly noted that governments need to 'avoid undermining' the work of journalists, stating that:

Strong safeguards should be developed to avoid future repeats of recent police raids on journalists, unlawful accessing of metadata to identify a journalist's source, and a spree of new national security legislation which criminalises journalistic activity.⁶⁵

Diaspora communities

- 7.59 This section considers how communities and individuals—in particular diaspora communities—can be empowered to improve their resilience against foreign interference through social media, as well as mitigating the impacts of disinformation, information campaigns, amplification and manipulation, propaganda and censorship.

- 7.60 The AHRC advised the committee of its concerns that foreign interference is increasing tensions and polarisation in Australia, writing that it:

... is increasingly disturbed by the role misinformation and disinformation plays in diminishing social cohesion, promoting distrust and division, and undermining principles of equality, respect and human dignity ...

Where social media is utilised by foreign actors to sow discontent and division in pursuit of their own agendas, disinformation can have a serious impact on the rights and freedoms of all Australians.⁶⁶

- 7.61 This view was supported by ASPI, which submitted that 'social media has created an unprecedentedly connected global community but this extensive reach has also allowed malign actors to intimidate, coerce and threaten violence beyond their borders, often with impunity and anonymity'.⁶⁷ It is also impacting on Australian's relationships with their family and friends overseas.⁶⁸

- 7.62 As outlined in Chapter 4, the Australian government has taken various steps to counter foreign interference through social media, including by way of social

⁶⁴ Human Rights Watch, *Submission 12*, p. 8. See also: Ms Melissa Harrison, *Submission 5: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 26; Badiucac, Private capacity, *Committee Hansard*, 21 April 2023, p. 37.

⁶⁵ Principle Co, *Submission 25: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 5.

⁶⁶ Australian Human Rights Commission, *Submission 9*, p. 7.

⁶⁷ Australian Strategic Policy Institute, *Submission 13*, pp. 3 and 15. See also: Dr William Stoltz, National Security College, Australian National University, *Submission 18*, pp. 17–18.

⁶⁸ Australian Tibetan Communities Association, *Submission 31*, pp. 2–3; Mr Kalsang Tsering, President, Australian Tibetan Community Association, *Committee Hansard*, 21 April 2023, pp. 24–26; Ms Vicky Xu, Senior Fellow, Australian Strategic Policy Institute, *Committee Hansard*, 21 April 2023, p. 34.

cohesion, community liaison and outreach programs, media campaigns, publication of fact sheets by Home Affairs, ASIO and Australian Federal Police (AFP).⁶⁹ Ms Sally Pfeiffer expanded on the work of Home Affairs:

... the Department of Home Affairs has a network of community liaison officers who worked very closely with culturally and linguistically diverse communities on a range of issues relating to Home Affairs activities, including some engagement on issues such as foreign interference. Those engagements are very important to us and we work very closely with those communities to make sure they have awareness of the potential for risks of foreign interference, and then what they can do to manage them.⁷⁰

7.63 In July 2023, Home Affairs advised that since February 2023, engagements relating to foreign interference had been conducted with the Arab, Cambodian, Chinese, Eritrean, Indian, Iranian, Vietnamese, Kurdish, Russian, Rwandan and Ukrainian communities.⁷¹

7.64 Mr Stephen Nutt, Commander of Special Investigations with the AFP told the committee of the importance of this type of work:

... my personal view is that the best strategy to defend against foreign interference is through high community and agency awareness and also knowledge of how to report it. If it's reported, we're able to understand it. And once we're able to understand it, we can work to disrupt and look at vulnerabilities that need to be corrected not only on individual case basis, but at more system level. So it's absolutely key.⁷²

7.65 This community outreach approach has been welcomed, with Dr Dowse from RAND Australia telling the committee:

I know that the Department of Home Affairs has been looking specifically at communities where English is not the first language, and I think that is a very intelligent priority because a lot of diaspora communities have their own sources of information which may not be mainstream and might not be traditional social media either. So I think understanding where those diaspora communities get their news and their information is important. It may change from diaspora to diaspora. I think understanding that is important if we're going to have a harmonious society, whether that's ideological or related to where the ethnic origins of portions of our society are. I think, to start with, that understanding where those potential sources of division might come from, including the sources of information and the influences ... and then understanding how you can balance that where there's concern about unfactual sources of information is an important

⁶⁹ See, for example: Mr Stephen Nutt, Commander, Special Investigations, Counter Terrorism and Special Investigations Command, Australian Federal Police, *Committee Hansard*, 12 July 2023, pp. 18 and 22.

⁷⁰ Ms Sally Pfeiffer, Department of Home Affairs, *Committee Hansard*, 12 July 2023, p. 7.

⁷¹ Department of Home Affairs, answers to questions on notice (no. 7), 12 July 2023 (received 18 July 2023).

⁷² Mr Stephen Nutt, Australian Federal Police, *Committee Hansard*, 12 July 2023, p. 22.

priority. So I was really happy to see that Home Affairs has got that as a priority.⁷³

- 7.66 The eSafety Commissioner also emphasised the targeted nature of the support it provides:

eSafety aims to provide support to a range of communities and groups, particularly to those most at risk of online harm. Our regulatory schemes can assist individuals who may be susceptible to foreign interference, such as diaspora groups, those with low digital literacy, and minority groups who may be the target of cyber abuse and illegal activity. These schemes intersect on a range of issues to provide multiple avenues of support.

In addition to targeted misogynistic abuse and gendered disinformation, women in the public eye who challenge autocratic leaders, traditional male power structures or human rights and gender issues tend to attract more organic and coordinated vitriol online.⁷⁴

- 7.67 Chapter 6 expanded on the steps platforms have undertaken to improve transparency and the awareness of disinformation within diaspora communities and the public. For example, platforms publishing enforcement and threat reports,⁷⁵ state media account labelling,⁷⁶ and Meta's development of a policy-focussed paper on misinformation and disinformation amongst diaspora groups with emphasis on Chinese language.⁷⁷
- 7.68 However, other witnesses argued that more needs to be done. ASPI argued that law enforcement and intelligence agencies should increase their community engagement to raise awareness, establish a reporting scheme to 'counter transnational repression', and reassure targeted individuals and groups.⁷⁸
- 7.69 The Australian Tibetan Communities Association argued for better consultation with civil society, and affected communities by government,⁷⁹ including regarding the development of new measures to counter foreign interference through social media and drafting new legislation.⁸⁰

⁷³ Dr Andrew Dowse, Director, RAND Australia, *Committee Hansard*, 20 April 2023, p. 30.

⁷⁴ eSafety Commissioner, *Submission 10*, p. [2].

⁷⁵ Meta Australia, *Submission 32*, pp. 15–16; Ms Emily Mosley, International Cyber Policy Centre Coordinator, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 23.

⁷⁶ TikTok, *Submission 30*, pp. 6 and 9; Mr Fergus Ryan, Analyst, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 20.

⁷⁷ Meta Australia, *Submission 32*, p. 14.

⁷⁸ Australian Strategic Policy Institute, *Submission 13*, p. 15.

⁷⁹ Australian Muslim Advocacy Network, *Submission 24*, pp. [18–19]; Australian Tibetan Communities Association, *Submission 31*, p. 5.

⁸⁰ Australian Tibetan Communities Association, *Submission 31*, p. 5.

7.70 Specifically, regarding the Chinese-Australian community, the Council on Middle East Relations urged the Australian Government to establish and maintain a presence on Chinese-language social media platforms in order to engage Chinese-Australians and Taiwanese-Australians and provide resources to assist these groups in identifying misinformation and disinformation.⁸¹ The China Policy Centre likewise encouraged such outreach to Chinese-Australians, stating that it would serve three key purposes:

First, it enables the better communication of government policy, strategy and priorities with the opportunity to hear community feedback ...

Second, regular and effective outreach by the Australian Government can assist with early identification of community concerns, and new challenges and threats. Chinese-Australians are the main targets of China's propaganda, misinformation, cyber surveillance, and censorship efforts through social media. Regular outreach provides an avenue to counter Chinese-language misinformation, especially in relation to government policy.

Third, the support of Chinese-Australians is crucial for an effective strategy addressing China's foreign interference efforts.⁸²

7.71 The AHRC noted challenges to rights to freedom from discrimination and freedom of expression citing harassment, surveillance and censorship of Australians by social media. The AHRC argued that:

Transparency is the key to ensuring that censorship (including extraterritorial censorship) does not unduly restrict the exercise of free speech in Australia. With respect to the last of these examples, the Commission would endorse the recommendation previously made by the ASPI International Cyber Policy Centre that governments 'should mandate that all social media platforms publicly disclose, in detail, all the content they censor and make it an offence to censor content where that has not been publicly disclosed to users'.⁸³

7.72 Dr Bruce Arnold of the University of Canberra submitted that an informed populace was in a significantly better position to be resilient. Dr Arnold observed that 'it is ... viable to emphasise community self-help, with participants in social media platforms being alert to the likelihood of misrepresentation and equipped to discern that statements are malicious'. Dr Arnold further noted that 'ultimately a savvy Australian population—with

⁸¹ Council on Middle East Relations, *Submission 25: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 4.

⁸² China Policy Centre, *Submission 4: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 3.

⁸³ Australian Human Rights Commission, *Submission 9*, p. 16. See also: Human Rights Watch, *Submission 12*, p. 8.

access to information through a public transparency regime—is the best defence against foreign interference and misbehaviour by domestic actors'.⁸⁴

7.73 Ms Shanthi Kalathil agreed, telling the committee:

We are really going to have to work on the long-term education and awareness raising of not just populations but different institutions of society ...

I think the Nordic countries, for instance, have several decades of history of building education and awareness about information into their educational systems from a young age. There are certainly examples we can look to around the world that can provide, if not a blueprint, some kind of indication about what might work and what might not work. So I think we need to do some serious looking at some of these examples from around the world to understand this problem better.⁸⁵

7.74 Regarding what practical activities individuals can undertake immediately, Principle Co encouraged Australians to:

- follow a wide spectrum of sources;
- seek our diversity of perspective, including by making sure that you are not just following voices that you naturally agree with; and
- ask questions, such as: who produced this content, what reaction is it seeking, and how did the information get to you?⁸⁶

⁸⁴ Dr Bruce Arnold, *Submission 7: Foreign Interference through Social Media inquiry (46th Parliament)*, p 7. See also John Abdelmalek, Kyron Johnson, Michael Barberio, and Mathew Bubica, with Dr James Scheibner, *Submission 40: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 20.

⁸⁵ Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, pp. 4–5.

⁸⁶ Principle Co, *Submission 25: Foreign Interference through Social Media inquiry (46th Parliament)*, p. 8.

Chapter 8

Committee view and recommendations

Overall committee view

- 8.1 In authoritarian states, citizens are subjected to government repression in the form of censorship, where people are restricted from freely discussing issues that would enable them to make fully informed social and political choices. Such censorship is anathema to the values of democratic states such as Australia. This provides authoritarian countries with an asymmetric advantage because they can readily censor narratives within their own country while simultaneously exploiting the openness of democratic societies to push their agendas offshore.
- 8.2 Because authoritarian governments cannot directly control the information environment in democratic states via overt censorship, they seek to control the information environment by flooding our online spaces with disinformation that skews public debate, undermines trust in our democratic institutions, establishes narratives that favour the interests of the perpetrating state and make it difficult for the casual observer to separate truth from fiction.
- 8.3 We cannot allow this rising authoritarianism to contaminate our democracy and undermine our social cohesion in the most challenging strategic environment since the World War II.
- 8.4 The Director General of the Australian Security Intelligence Organisation (ASIO) recently declared that Australia is facing an unprecedented challenge from foreign interference and espionage, and that he is not convinced that we fully appreciate the damage that it inflicts on our security, our democracy, our economy and our social fabric.¹
- 8.5 Because social media has become such a dominant form of communication it is also a dominant vector for foreign interference via disinformation, coordinated inauthentic behaviour networks and transnational repression, which carries profound consequences for our liberal democracy.
- 8.6 Whether we like it or not, modern social media platforms are not just a mode of communication—in democratic states they have also become the new public square, where important issues are debated, interrogated and resolved. They help shape public opinion and, ultimately, the choices democracies make. For this reason they are a highly attractive domain for our potential adversaries,

¹ Mike Burgess Director-General of Security, Australian Security Intelligence Organisation, *Director-General's Annual Threat Assessment*, 21 February 2023.

who engage in information operations on these platforms to influence these decisions.

- 8.7 Protecting people's rights to participate in our democracy in the digital town square is a balancing act. As the Australian Human Rights Commission (AHRC) raised with this committee, social media can be used for purposes that both strengthen or harm our democracy and values.² The difficult task for governments is to ensure any policy responses strike the right balance and protect the foundations of our democracy. All Australians must have their free speech protected while also preserving the fundamental right to participate in a democratic society that is free from covert influence and manipulation.
- 8.8 This balancing act is even more precarious when the platform in question is headquartered in a country with a form of government that is fundamentally incompatible with our own. When asked why should a liberal democracy be uncomfortable with a platform like WeChat being the dominant source of information for a diaspora community if it is potentially controlled by a foreign government, Dr Seth Kaplan advised the committee that 'instead of your democracy being a debate among people who live in your country, there's an additional voice that plays a large part in the conversation, and that voice is controlled by a foreign government that does not have your best interests at heart ... that [is] the most clear danger'.³ The committee heeds this warning, and believes we must take action now to shine a light on these covert, malign sources of influence in our democracy to make Australia a harder target for cyber-enabled foreign interference peddlers.
- 8.9 Foreign interference does not only impact our public discourse. Many people living in Australia are not free of the long hand of their repressive former governments, reaching across the seas to continue to engage in acts of intimidation, harassment and violence including through social media. As Chinese-Australian artist and activist Badiucao testified to this committee, in relation to WeChat being used by the Chinese government for disinformation and propaganda purposes, we cannot allow a situation in which foreign authoritarian governments exploit social media platforms to export their censorship in a manner that is fundamentally at odds with our liberal democratic values and endangers our national security.⁴ Australia must protect those people, who deserve to live a life free from fear, and they deserve the protection of the Australian Government when malicious actors try to take away that freedom that all Australians enjoy.

² Australian Human Rights Commission, *Submission 9*, p. 3.

³ Dr Seth Kaplan, Private capacity, *Committee Hansard*, 20 April 2023, p. 12-13.

⁴ *Committee Hansard*, 21 April 2023, p. 35.

- 8.10 This is not a partisan issue. Liberal democracies around the world agree that foreign interference and information manipulation, particularly from authoritarian states, is one of the greatest contemporary challenges to democracy.
- 8.11 As outlined by the AHRC, social media can be used to either strengthen or undermine democracy. Getting the settings right requires a clear-eyed, non-partisan approach to confront the dangers our nation faces via the weaponisation of social media to damage our democracy.
- 8.12 We must also recognise the speed at which this challenge is moving as technology evolves exponentially. We can no longer afford to react only once the impacts of foreign interference become apparent, because at that point it is too late for countermeasures to be effective. We must learn to anticipate future risks to our democracy and social cohesion.
- 8.13 That means our countermeasures must be agile and our regulatory framework adaptable to emerging technologies. Legislative settings must be platform and technology agnostic, based on the principles of safety and transparency with clear benchmarks for external oversight, and undergirded by meaningful sanctions when transparency principles are breached.

Platform transparency

- 8.14 Transparency is a foundational principle of any democracy. It is a key ingredient to build accountability and trust, and arguably the strongest antidote to disinformation in a system that seeks to preserve free speech. Australians must be able to trust that the information they see on social media platforms has not been manipulated to serve the strategic interests of a foreign government whose values and interests may run counter to our own.
- 8.15 Democracy also relies on the polity being confident that accurate and truthful information is not being withheld through censorship, and that people are able to engage in free and frank discussion. However, the use of coordinated inauthentic behaviour (CIB) to distribute disinformation is neither free nor frank, as it leverages automatic processes—often coordinated from offshore—to amplify the voice of an interested party and create the illusion of support on a much larger scale. As one expert succinctly put it, *why should a bot have the same free speech rights as me?*
- 8.16 The committee heard from numerous experts on cyber security, human rights, politics, and community cohesion, all of whom were consistent in their message that the lack of transparency about the way social media platforms operate creates a permissive environment for covert social manipulation that often goes undiscovered.
- 8.17 Australia recognised the importance of transparency in strengthening our democracy via the introduction of the *Foreign Influence Transparency Scheme*

(FITS) in 2018. The FITS requires foreign actors to register their lobbying and communications activities in Australia, and this scheme has since been replicated by other nations who have looked to us as a leader on these issues.

- 8.18 Following a request from the Australian Government in 2020, the Digital Industry Group Inc (DIGI)—working in conjunction with industry—released the 2021 *Australian Code of Practice on Disinformation and Misinformation* (voluntary code), which committed a diverse set of technology companies to take steps to reduce the risk of online misinformation causing harm to Australians. Despite its admirable intent, there is little evidence to suggest the voluntary code has been effective in combating foreign state disinformation, which remains rife on both western-headquartered social media platforms and those from authoritarian states.
- 8.19 The Australian Government has released an exposure draft of the Communications Legislation Amendment (Combating Misinformation and Disinformation) Bill 2023 (the Bill), which gives the Australian Communications and Media Authority (ACMA) powers to gather information from platforms on their records regarding misinformation and disinformation; request industry develops a code of practice; and allows the ACMA to create and enforce industry standards should the code be deemed ineffective.
- 8.20 Although the draft bill was raised during public hearings of the Select Committee, we did not conduct a formal inquiry into the bill. For that reason, it would not be appropriate for the committee to express a view about the merits or otherwise of the Australian Government's proposed approach.
- 8.21 Regardless of whether the draft bill proceeds or not, the committee believes that the increasing risk that foreign interference and disinformation poses to Australia's democratic institutions, values and way of life, means that there is a pressing need for additional action to counter the efforts of authoritarian states that seek to weaponise social media platforms against liberal democracies like Australia.
- 8.22 The committee agrees with evidence that censorship and the reporting of alleged misinformation can itself present a risk of foreign interference.
- 8.23 The AHRC noted 'increased examples of extra-territorial censorship, where governments seek to suppress speech outside of their national borders'. ASIO advised that acts such as these 'could become foreign interference if they involve the hidden hand of a foreign state'.⁵
- 8.24 Foreign government officials pressuring social media companies to make censorship content removal decisions which are in their political or strategic

⁵ Australian Human Rights Commission, *Submission 9*, pp. 4 and 15.

interests but contrary to Australia's democratic processes and national interests represents a foreign interference risk.

- 8.25 While some platforms do report formal legal requests made by government and any action taken as a result, is the removal or restriction of content after informal or non-official requests from foreign government officials, particularly where it is later claimed by the platform that the content breached their policies, that is particularly lacking in transparency. As acknowledged by Twitter, this type of action reduces public trust.
- 8.26 Additionally, though, if content removal, restriction or visibility filtering occurs after an informal request from a foreign government which is not disclosed by platforms, this can result in an unacceptable form of foreign interference in Australian public debate and discussion.
- 8.27 Decisions made by social media companies to censor or remove content on the grounds that it is allegedly 'misinformation' or causes 'harm' can adversely affect public discourse in our democracy. This was particularly demonstrated by Meta's decisions during the pandemic to restrict content on its platform discussing the theory that a laboratory accident might have been involve in the origins of the virus as 'misinformation', despite the fact that we now know that the US Intelligence Community was asked by the Biden administration to investigate the origins of the virus and are divided in their findings on this issue. The Australian public had no visibility over how such decisions were made and whether there was pressure from foreign governments to remove such content, and this demonstrates that less censorship, rather than more, is the safest option for our democracy.
- 8.28 Current transparency measures by social media companies do not adequately cover pressure applied by government officials to censor content where this pressure is applied outside of formal legal channels.
- 8.29 There is wide scope for foreign government officials to pressure social media staff to make a finding that content that they wish to have removed should be interpreted as being in breach of the platform's rules, despite not having been deemed to be so prior to the government's request.
- 8.30 This issue goes directly to the concerns about censorship raised by submitters and witnesses that social media platforms should be required to be fully transparent about the content they censor or visibility filter in response to requests from foreign governments, whether as a result of a legal process or through other channels.
- 8.31 Under current policies, decisions to censor content following requests from foreign governments can be obscured by statements from platforms that the content breached their content policies.

- 8.32 There is currently an unacceptable risk of staff at social media companies making content moderation decisions which affect Australian political discourse and democratic processes under pressure from foreign government officials, without this being adequately disclosed to the Australian public.
- 8.33 Several experts who testified before the committee recommended that the best path forward is to introduce enforceable transparency obligations that social media companies must meet to continue operating in Australia.
- 8.34 Dr Seth Kaplan recommended a 'step-by-step approach' where we say 'these are the rules that function in a democracy, these are the things we expect and these are the penalties' and serious non-compliance could be met with enforcement measures, including up to a ban of the social media application.⁶
- 8.35 Mr Albert Zhang from the Australian Strategic Policy Institute also favoured 'regulation or at least a discussion about how we standardise and create better reporting mechanisms to increase transparency', and Mr Fergus Ryan called for 'legislation that deals with any other emerging apps that may come out of countries like China'.⁷
- 8.36 Similarly, Australian cybersecurity firm CyberCX called for 'mandatory compliance and report frameworks for social media platforms' so that the government has the final say on managing risks to our democracy.⁸
- 8.37 Finally, the AHRC supported establishing 'clear and mandatory requirements, and pathways, for social media organisations to report suspected foreign interference' and to require social media platforms to publicly disclose the content that they censor and make it an offence to censor content where that has not been publicly disclosed to users.⁹
- 8.38 Given this, the committee recommends an approach that favours transparency over censorship, whereby platforms are given reasonable hurdles to meet and it is incumbent on them to take reasonable steps to inform Australians about the origin, and, where possible, the intent of the content they are exposed to so they can make up their own minds about its merits. This serves as a reasonable alternative to a more heavy-handed approach, wherein decisions about what constitutes allowable speech are outsourced to tech platforms—most of which are headquartered overseas—in the name of user 'protection'.
- 8.39 For example, content which has been published by a proxy of an authoritarian state, such as state media broadcasters like Russia's RT, or China's Xinhua,

⁶ Dr Seth Kaplan, Private capacity, *Committee Hansard*, 20 April 2023, p. 16.

⁷ Mr Fergus Ryan, Analyst, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 21

⁸ CyberCX, *Submission 16*, p. 4.

⁹ Australian Human Rights Commission, *Submission 9*, p. 9.

would be labelled as such, instead of being censored. Informed of the origins of this content, users can decide for themselves how much weight to award it. Some social media platforms already do this, while others have never done so, or recently ceased doing so.

- 8.40 However, transparency should not be restricted to information that users see, it must also be for information that users do not see due to censorship or other forms of visibility manipulation. Australian laws should discourage censorship of political discussion and public policy debate by social media platforms outside of very clearly defined legal processes.
- 8.41 Under this transparency-led model, platforms who fail to meet these reasonable standards would be fined, while repeated non-compliance could result in a ban given the harmful impact this conduct would have on our democracy.
- 8.42 The committee therefore recommends the Australian Government immediately create a system of enforceable minimum transparency standards that all social media platforms operating in Australia must meet, underpinned by appropriate sanctions to ensure compliance up to and including banning platforms from operating within Australia.

Recommendation 1

- 8.43 **The committee recommends the Australian Government require all large social media platforms operating in Australia to meet a minimum set of transparency requirements, enforceable with fines. Any platform which repeatedly fails to meet the transparency requirements could, as a last resort, be banned by the Minister for Home Affairs via a disallowable instrument, which must be reviewed by the Parliamentary Joint Committee on Intelligence and Security.**
- 8.44 **Requirements should include, at minimum, that all large social media platforms:**
- **must have an Australian presence;**
 - **must proactively label state affiliated media;**
 - **must be transparent about any content they censor or account takedowns on their platform;**
 - **must disclose any government directions they receive about content on their platform, subject to national security considerations;**
 - **must disclose cyber-enabled foreign interference activity, including transnational repression and surveillance originating from foreign authoritarian governments;**
 - **must disclose any takedowns of coordinated inauthentic behaviour (CIB) networks, and report how and when the platform identified those CIB networks;**

- must disclose any instances where a platform removes or takes adverse action against an elected official's account;
- must disclose any changes to their platform's data collection practices or security protection policies as soon as reasonably practicable;
- must make their platform open to independent cyber analysts and researchers to examine cyber-enabled foreign interference activities;
- must disclose which countries they have employees operating in who could access Australian data and keeps auditable logs of any instance of Australian data being transmitted, stored or accessed offshore; and
- must maintain a public library of advertisements on their platform.

Platforms headquartered in authoritarian states

- 8.45 Experts in cyber security and foreign interference sent a clear and consistent message to the committee: social media platforms that originate from authoritarian states present an additional layer of risk. CyberCX warned the committee that the collection and aggregation of the personal information of millions of Australians and the capacity for malign foreign actors to manipulate content consumed by Australians at scale is a heightened risk for platforms that are linked to authoritarian governments, including TikTok and WeChat.¹⁰ As they pointed out, Chinese government authorities operate 'without the oversight and transparency mechanisms of rule-of-law democracies', and therefore it is clear to the committee that platforms headquartered in authoritarian states deserve even greater scrutiny because of the heightened risks to our democracy and citizens.
- 8.46 It is not merely that authoritarian states tend to place less emphasis on personal privacy and data protection. It is that those authoritarian states have deliberately—themselves or by proxy—designed social media platforms that can both obscurely harvest vast swathes of user data while also covertly manipulating the information environment to serve the interests of the intervening state. Dr William Stoltz from the Australian National University's National Security College advised this committee that information campaigns can be weaponised to 'flood the information sphere' with multiple and even contradictory narratives that sow confusion or discord, distract attention, and to encourage the target audience to question the authenticity of other information and induce wider cynicism.¹¹
- 8.47 ASIO highlighted the additional security concerns that authoritarian governments 'are able to direct their country's institutions—including media,

¹⁰ CyberCX, *Submission 16*, p. 5.

¹¹ Dr William Stoltz, National Security College, Australian National University, *Submission 18*, p. 9.

businesses and society—to support intelligence or foreign policy objectives in ways which are not acceptable in a democracy'.¹²

- 8.48 The committee is alarmed by this rising authoritarianism creeping into our society through the digital domain, and we must be alert and ready to respond to these grey zone tactics that fall short of war but still corrode our democracy and sovereignty.
- 8.49 These platforms' ability to gain and maintain our attention through opaque algorithms and relentlessly collect user data did not develop by accident. Each platform's commitment to these features goes well beyond a simple commercial imperative as failure to comply with the will of an authoritarian government is often an existential decision for platforms headquartered in these countries. Consequently, these tactics are vigorously defended by both the platforms themselves as well as their authoritarian governments who have a vested interest in preserving access to harvested data from democratic nations. It is little wonder that China's Ambassador to Australia, Xiao Qian, protested the Australian Government's decision on 4 April 2023 to ban TikTok from government-owned devices and cease using technology from Chinese-manufactured companies which are ultimately beholden to the demands of the Chinese Communist Party (CCP).¹³
- 8.50 The committee's concerns are echoed across the globe. As early as 2015, the European Council publicly stressed 'the need to challenge Russia's ongoing disinformation campaigns' and called for 'an action plan on strategic communication'.¹⁴ A recent joint address by the heads of Security Service MI5 (United Kingdom) and the Federal Bureau of Investigation (United States) noted that the CCP is covertly applying pressure across the globe via a coordinated campaign on a grand scale that involves planned, professional activity in support of a decades-long strategic contest.¹⁵
- 8.51 In the case of TikTok and WeChat, both platforms originate from China, where national security laws such as Article 7 of the National Intelligence Law of 2017 require those platforms, and their employees, to assist national security agencies with any request they may make, and furthermore, to keep those requests secret. As Ms Shanthi Kalathil testified to this committee, 'were the [Chinese] state to go to [ByteDance and Tencent] with certain demands, they would be unable to

¹² Australian Security Intelligence Organisation, *Submission 2*, p. 4.

¹³ Karen Barlow, '[China 's ambassador to Australia slams speculation of TikTok, surveillance device spying](#)', *Canberra Times*, 18 May 2023.

¹⁴ European Council conclusions, 20 March 2015, [EUCO 11/15](#), p. 5.

¹⁵ Security Service MI5, *Joint Address by MI5 and FBI Heads*, 6 July 2022, [www.mi5.gov.uk/news/speech-by-mi5-and-fbi](#) (accessed 14 July 2023).

legally or in any other capacity resist those demands'.¹⁶ The committee is deeply concerned that the consequence of this extrajudicial direction is that social media companies that are ultimately beholden to the CCP have unfettered access to the personal data of millions of Australians that could ultimately end up in the hands of a foreign intelligence service.

- 8.52 Throughout this inquiry, both WeChat and TikTok have been reluctant participants in this parliamentary scrutiny of social media platforms—a scrutiny that is itself an expression of Australia's democracy. This reluctance to participate speaks volumes about the respect those platforms hold for Australian democratic processes, and stood in stark contrast to the more cooperative disposition of platforms headquartered in western countries who recognise the fundamental importance of the checks and balances inherent in democratic systems.
- 8.53 The committee notes that WeChat repeatedly declined multiple invitations to participate in a public hearing on grounds it does not have a legal presence in Australia, ignoring that the invitation allowed them to participate via videoconference from any location in the world—an option other witnesses utilised. As Chair of the Select Committee, Senator Paterson sent an open letter on 4 July 2023 to WeChat urging them to reconsider their refusal to appear at a public hearing. While WeChat reiterated its stated intention to 'working collaboratively with Australian regulators and authorities' and said that it remained 'committed to providing responsive information to the committee in writing', its blanket refusal to front up in an open forum demonstrates to the Australian public that WeChat is not genuinely committed to being held accountable for the allegations of censorship, surveillance and foreign interference at the hands of the CCP that are rife on its platform.¹⁷ WeChat's written responses, delivered on 26 July 2023, to the committee's 53 questions on notice, do nothing to assuage our strongly held concerns. WeChat's responses demonstrate a non-genuine effort to assist the committee with answers that completely lack credibility and are widely contradicted by the evidence of independent experts.
- 8.54 TikTok was similarly reluctant to participate, requiring the committee to remind them of its powers to compel any Australian-based employee to appear at a hearing. Once in attendance, the committee found TikTok engaged in a determined effort to obfuscate and avoid answering simple questions about their platform's operations and its links to their parent company, ByteDance, and its relationship with the CCP.

¹⁶ Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, p. 3.

¹⁷ Senator James Paterson, 11 July 2023, <https://twitter.com/SenPaterson/status/1678557229883207681> (accessed 29 July 2023).

- 8.55 On all the available evidence, including TikTok's admission that the majority of ByteDance employees are based in China, the committee does not accept TikTok's statement that 'ByteDance operates as a global company without an officially designated headquarters.' This claim has been contradicted by TikTok and ByteDance's own public statements including in court-filings in the US.¹⁸ It is clear that TikTok's parent company, ByteDance, is headquartered in China where the majority of its employees are based, and is therefore subject to the Chinese Government's laws including the 2017 National Intelligence Law. As TikTok witnesses reluctantly admitted, those China-based employees can remotely access Australian user data, and can even make changes to the algorithm.
- 8.56 TikTok's obfuscation continued with their responses to questions on notice, which were not appropriately answered. TikTok told the committee that 'data is protected, kept and logged in our company'¹⁹ but were unable to give a number on how often Australian user data had been accessed by employees in China, and TikTok said it did not have specific numbers but would take that on notice. TikTok's follow-up answer was not enlightening either; TikTok failed to quantify the number of times Australian user data had been accessed by mainland China. The only reasonable conclusions the committee can reach is that TikTok does not track and log this data access in the way it first suggested to the committee and has failed to correct the record, or it does do so but is refusing to provide the information because it would be a shockingly large number. Neither prospect reflects well on the company, its officers or its commitment to comply with Australian law.
- 8.57 Again, this is not an issue that is isolated to Australia. Other nations have sought to engage with TikTok about ongoing security concerns they hold with the practices of the platform, and have also found TikTok to be reluctant participants who were evasive and misleading under questioning. In their letter to the US Federal Trade Commission, US senators Mark R. Warner (D-VA) and Marco Rubio (R-FL) criticised the 'repeated misrepresentations by TikTok

¹⁸ John Garnaut et al, *Submission 34*, p. 39 citing TikTok Inc v Donald J Trump, Plaintiffs ' Notice of Filing, 10 November 2010: 'The parties [TikTok Inc and ByteDance Ltd] did not submit the Musical.ly transaction to CFIUS for review in 2017 because ByteDance was a Chinese-headquartered company and Musical.ly was also a Chinese-headquartered company', p. 12. www.scribd.com/document/483797602/TikTok-asks-U-S-federal-appeals-court-to-vacate-U-S-divestment-order#.

¹⁹ Ms Ella Woods-Joyce, Acting Director of Public Policy, Australia and New Zealand, and Mr Will Farrell, Security Officer, TikTok US Data Security, TikTok, *Committee Hansard*, 11 July 2023, pp. 23–24.

concerning its data security, data processing, and corporate governance practices'.²⁰

- 8.58 It is also telling that all social media platforms who appeared before the committee stated that they found and removed CIB that sought to influence Australia. In contrast, TikTok declared that there was no such CIB on its platform.²¹ The committee holds this declaration in high suspicion.
- 8.59 Concerningly, in answers to questions on notice, TikTok Australia admitted that its much-vaunted Project Texas, designed to supposedly protect American user data, and Project Clover, which purports to protect European user data, has no Australian equivalent. Although widely criticised by independent experts—including Ms Shanthi Kalathil²² and the US Federal Communications Commissioner Mr Brendan Carr²³ who testified before this committee—as insufficient to protect user data, TikTok in these jurisdictions at least feels compelled to offer this fig-leaf. It is telling that no similar proposal exists for Australian users. Australia cannot again be left behind, and must be included in any solution to the problem posed by ByteDance's ownership of the app.
- 8.60 The committee notes the ongoing exploration of options in relation to ownership of TikTok in the US, which are centered on divesting ownership away from a company that is beholden to the national security laws of the CCP, thereby severing TikTok's obligations to cooperate with China's intelligence apparatus. Should the US Government take action to force ByteDance to divest ownership of TikTok, the Australian Government should take advantage of that move to implement similar requirements in Australia.

Recommendation 2

- 8.61 The committee recommends that, should the United States Government force ByteDance to divest its stake in TikTok, the Australian Government review this arrangement and consider the appropriateness of ensuring TikTok Australia is also separated from its ByteDance parent company.**

Apps on government devices

- 8.62 On 4 April 2023, the Australian Government issued a directive under the *Protective Security Policy Framework* (PSPF) that TikTok could not be installed on any Australian Government-issued devices due to the serious espionage risk.

²⁰ Senator Mark R. Warner (US), '[Warner, Rubio call for Investigation into TikTok in Light of Revelations about Chinese Communist Party 's Potential Access to U.S. Data](#)', 5 July 2022.

²¹ Ms Ella Woods-Joyce, TikTok, *Committee Hansard*, 11 July 2023, p. 20.

²² Ms Shanthi Kalathil, Private capacity, *Committee Hansard*, 20 April 2023, p. 4.

²³ Mr Brendan Carr, Commissioner, US Federal Communications Commission, *Committee Hansard*, 20 April 2023, pp. 10–11.

- 8.63 Ms Abigail Bradshaw, the Deputy Director General of the Australian Signals Directorate and Head of the Australian Cyber Security Centre, outlined the rationale for the ban in compelling evidence to the committee. Ms Bradshaw detailed the extensive data collection practices of TikTok, including its attempts to access data held by other applications on a device, and noted the company was subject to the extrajudicial direction of the Chinese Government. When asked about TikTok's public statements that it has never been asked to hand over its data to the Chinese Government, Ms Bradshaw advised that she had 'not seen technical controls that would provide a basis for technical advice that the risks of sharing data are adequately mitigated'.²⁴
- 8.64 While the ban of TikTok from Australian Government devices is a promising first step, there are still security gaps that must be addressed. For example, the Attorney-General's Department (AGD) noted that while the PSPF also applied to government contractors, AGD did not have oversight over whether departments had turned their minds to ensuring contractors either knew about or were adhering to the TikTok ban. If TikTok is not safe to be on the device of a government employee, it is not safe to be on the device of a government contractor who has access to similarly sensitive information.
- 8.65 During the inquiry it emerged that several major consulting firms took the decision to ban TikTok from their employee's work-issued devices following correspondence from the Shadow Minister for Home Affairs and Cyber Security.²⁵
- 8.66 WeChat poses a similar data security risk to TikTok and should be added to the PSPF ban, with appropriate exemptions available on a case-by-case basis provided sufficient security mitigations are deployed, as is the case with TikTok. Additional research on other platforms should be undertaken, with a view to developing more detailed guidance on the installation of any similar social media platforms onto devices that can access sensitive government data and information.
- 8.67 Critical infrastructure entities regulated under the *Security of Critical Infrastructure Act 2018* (SOCI Act) especially those designated as Systems of National Significance by the Minister for Home Affairs, are recognised as providers of essential services to the Australian people. Under the SOCI Act, entities are required to take steps to protect themselves from a range of risks, including risks to cyber security. Evidence provided by the Department of Home Affairs (Home Affairs) during Senate Estimates indicated it was an option

²⁴ Ms Abigail Bradshaw, Deputy Director-General, Australian Signals Directorate, *Committee Hansard*, 12 July 2023, p. 3.

²⁵ Senator James Paterson, Committee Chair, and Ms Sarah Chidgey, Deputy Secretary, National Security and Criminal Justice, Attorney-General's Department *Committee Hansard*, 12 July 2023, pp. 20–21.

available to the government to direct these entities to take reasonable steps to mitigate the risk of apps like TikTok.²⁶

- 8.68 Applications like TikTok and WeChat illustrate the broader risk to sensitive government information from software and hardware posed by high-risk vendors, particularly those subject to the control of authoritarian foreign governments. It was clear during the inquiry that there is currently no entity within government with central policy responsibility for mapping, assessing and mitigating the risks posed by these vendors. Too often, government is reactive in its approach to high-risk technologies, only taking action to ban software or restrict hardware after it has generated public controversy. We need to move to a proactive setting which considers the risk of emerging technologies before they are widely installed by government users and subsequently have to be removed or have mitigations applied at great cost and inconvenience.

Recommendation 3

- 8.69 **The committee recommends the Australian Government extend, via policy or appropriate legislation, directives issued under the *Protective Security Policy Framework* regarding the banning of specific applications (e.g. TikTok) on all government contractors' devices who have access to Australian government data; and**
- 8.70 **The Minister for Home Affairs should review the application of the *Security of Critical Infrastructure Act 2018*, to allow applications banned under the *Protective Security Policy Framework* to be banned on work-issued devices of entities designated of Systems of National Significance.**

Recommendation 4

- 8.71 **The committee recommends the Australian Government consider extending the *Protective Security Policy Framework* directive banning TikTok on federal government devices to WeChat, given it poses similar data security and foreign interference risks.**

Recommendation 5

- 8.72 **The committee recommends the Australian Government continues to audit the security risks posed by the use of all other social media platforms on government-issued devices within the Australian Public Service, and issue general guidance regarding device security, and if necessary, further directions under the *Protective Security Policy Framework*.**

²⁶ Mr Michael Pezzullo AO, Secretary, and Mr Hamish Hansford, Deputy Secretary, Cyber and Infrastructure Security Centre, Department of Home Affairs, Senate Legal and Constitutional Affairs Legislation Committee, *Estimates Committee Hansard*, 22 May 2023, pp. 67–68.

Recommendation 6

8.73 The committee recommends the Australian Government establish a national security technology office within the Department of Home Affairs to map existing exposure to high-risk vendors such as TikTok, WeChat and any similar apps that might emerge in the future. It should recommend mitigations to address the risks of installing these applications, and where necessary, ban them from being installed on government devices.

Building the capacity of government

Lead agency

8.74 The committee considers that the Australian Government must urgently increase its expertise and technical capability in combatting foreign interference through social media to address current and emerging threats.

8.75 In this report, the committee has mapped the departments, agencies and taskforces involved in addressing foreign interference through social media and created a visual diagram showing the complexity and diffusion of responsibility created by these arrangements. This was further highlighted in discussions with Home Affairs, who told the committee that despite having responsibility to run the Counter Foreign Interference Coordination Centre, it was not a member of the Counter Foreign Interference Taskforce.²⁷

8.76 While a range of agencies contribute their specialist knowledge to track, analyse and counter foreign interference, there is a general lack of accountability because no single entity is accountable for the outcomes. A dedicated body is needed to coordinate government efforts and serve as a one-stop shop for individuals and private sector stakeholders to report and seek advice about suspected foreign interference through social media. This body should also serve a public outreach function and regularly publish advice to support companies and individual recognise and appropriately respond to foreign interference activity.

8.77 The AHRC, the Australian Strategic Policy Institute and CyberCX all testified to this committee that the Australian Government should nominate a lead government entity that is responsible for countering cyber-enabled foreign interference.²⁸

8.78 The committee notes that this proposed body, and existing agency efforts, need to be adequately resourced. Despite an announcement on 14 February this year that Home Affairs and ASIO have been tasked with a new community outreach

²⁷ Ms Sally Pfeiffer, Acting First Assistant Secretary, Counter Foreign Interference, Department of Home Affairs, *Committee Hansard*, 12 July 2023, p. 12.

²⁸ Australian Human Rights Commission, *Submission 9*, p. 8; CyberCX, *Submission 16*, p. 4; Mr Albert Zhang, Analyst, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 21.

program to counter foreign interference, Home Affairs informed the committee it was not given any new resources to undertake this work. It is vital that Australia's frontline agencies in the fight against foreign interference are adequately resourced so that the acquittal of their broader functions is not weakened or jeopardised due to resources being spread too thin.

- 8.79 The committee further notes the recent agreement between the European Union and the US to use a common methodology for identifying, analysing and countering foreign interference. By using the DISARM framework, STIX2 standard and the OpenCTI platform, information between the two regions will be shared more efficiently, effectively and with a greater level of detail. A lead agency in Australia should quickly move to adopt the same standards and join this coalition so that we can leverage the learnings and scale of likeminded partners while sharing our own experiences to inform best practice.

Recommendation 7

- 8.80 The committee recommends the Australian Government designate an entity with lead responsibility for whole-of-government efforts to counter cyber-enabled foreign interference, with appropriate interdepartmental support and collaboration, resources, authorities and a strong public outreach mandate.**

Cyber security strategy should include foreign interference

- 8.81 Home Affairs is currently developing the *2023-2030 Australian Cyber Security Strategy*. Earlier this year Home Affairs published a discussion paper seeking views to inform the final strategy, however despite the discussion paper noting that cyber technology provides a conduit for 'crime, foreign interference, espionage, disinformation and misinformation', none of these issues are addressed in the suggested 'core policy areas that the Expert Advisory Board expects will be addressed in the Strategy'.²⁹ The committee is concerned that this area of risk is not being appropriately addressed within the strategy, which provides a logical mechanism to address the risk of cyber-enabled foreign interference as part of broader efforts to uplift Australia's national cyber resilience.

Recommendation 8

- 8.82 The committee recommends the Australian Government address countering cyber-enabled foreign interference as part of the *2023–2030 Australian Cyber Security Strategy*.**

²⁹ Australian Government, [2023-2030 Australian Cyber Security Strategy: Discussion Paper](#), pp. 6 and 16.

Magnitsky sanctions

8.83 There are existing provisions within the *Autonomous Sanctions Act 2011* which allow the Australian Government to impose targeted financial sanctions and travel bans against perpetrators and beneficiaries of prohibited behaviours and actions. The scheme allows the government to create sanctions that are either country-specific or thematic. Thematic sanctions can currently be imposed for:

... the proliferation of weapon of mass destruction; threats to international peace and security; malicious cyber activity; serious violations or serious abuses of human rights; activities undermining good governance or the rule of law, including serious corruption; and serious violations of international humanitarian law.³⁰

8.84 The committee recommends that the scope of the Australia's Autonomous Sanctions regime should be clarified to ensure include foreign interference through social media, via amendments to the Act if necessary. This will serve as a deterrent to foreign states seeking to conduct foreign interference in Australia, and will allow Australia to issue sanctions and attributions in concert with likeminded partners for foreign interference attempts as we already have the ability to do for cyber-attacks.

Recommendation 9

8.85 The committee recommends the Australian Government clarify that Magnitsky-style cyber sanctions in the *Autonomous Sanctions Act 2011* can be used to target cyber-enabled foreign interference actors, via legislative amendment if necessary, and ensure it has appropriate, trusted frameworks for public attribution.

Capacity to lay charges for foreign interference

8.86 The committee heard from a range of community groups about the impacts that foreign interference has on the lives of many culturally diverse people in Australia. These groups and individuals make numerous reports to the National Security Hotline on specific instances of interference, threats, harm and campaigns of harassment, many of which are conducted using social media platforms.

8.87 Despite these numerous reports, the Australian Federal Police (AFP) reported to the committee that not a single person has been charged with offences relating to foreign interference via a social media platform under the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (the Espionage Act). The AFP noted there is a very high bar to laying such charges, which requires either a foreign principal or a proxy of a foreign

³⁰ Department of Foreign Affairs and Trade, *Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021*, www.dfat.gov.au/news/news/autonomous-sanctions-amendment-magnitsky-style-and-other-thematic-sanctions-act-2021 (accessed 24 July 2023).

principal to be undertaking the action. As such, the Espionage Act should be reviewed to ensure the settings are correct for the current operating environment.

- 8.88 Further, the Law Council of Australia (Law Council) submitted that the intention was for offences introduced by the Espionage Act into the *Criminal Code Act 1995* to be applied to conduct where social media is used to exert the influence on behalf of a foreign actor by deceptive or covert means. However, the Law Council queried the utility of these provisions being used against instances of foreign interference through social media given 'the challenges that exist in relation to successfully investigating and prosecuting persons who commit this offence when the 'conduct' occurs outside Australia'.³¹
- 8.89 The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is currently reviewing the *Foreign Influence Transparency Scheme*. Despite evidence put to the committee that these reforms should be considered as part of a package with the *Espionage and Foreign Interference Act 2018*, the PJCIS is not required to complete a review of the Espionage Act, and has not been referred an inquiry to do so. The scheduled review of the Espionage Act by the Independent National Security Legislation Monitor (INSLM) is not likely to be completed in this term of the INSLM due to other review priorities.

Recommendation 10

- 8.90 The committee recommends the Australian Government refer the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* to the Parliamentary Joint Committee on Intelligence and Security for review, with particular reference to the Act's effectiveness in addressing cyber-enabled foreign interference.**

Artificial intelligence: an emerging threat

- 8.91 The committee is alarmed at the increasing national security risks associated with the potential weaponisation of artificial intelligence (AI) technologies by malicious actors. These concerns have sharply increased with the advent of generative AI tools such as ChatGPT and Midjourney, which can be used to generate content at a speed and scale we have never seen before.
- 8.92 Expert witnesses told the committee that AI will exponentially increase the volume of disinformation and foreign agents engaging in CIB. Mr David Robinson from Internet 2.0 warned the committee that 'because of artificial intelligence we assess time is not on our side' and that AI is 'increasing the effectiveness of influence and disinformation campaigns against elections',

³¹ Law Council of Australia, *Submission 27*, pp. 2-3.

cautioning that we may not be able to reverse the loss of trust our system will suffer.³²

- 8.93 The Department of Industry, Science and Resources is currently leading the Australian Government's public consultation on the responsible use of AI. The Government's discussion paper on 'safe and responsible AI in Australia' specifically excludes consideration of the national security implications of AI. This is one of the most pressing areas of concern today.³³ The Australian Government must urgently address the national security implications in our policy response to AI.

Recommendation 11

- 8.94 The committee recommends the Australian Government investigate options to identify, prevent and disrupt artificial intelligence (AI)-generated disinformation and foreign interference campaigns, in addition to the Government's Safe and Responsible AI in Australia consultation process.**

Intelligence briefings

- 8.95 The committee heard from both social media platforms and government agencies about the importance of collaborative relationships between the two sectors. However, cooperative platforms were often stymied in their ability to take targeted action because they lack the threat intelligence that could assist them in focusing their search for disinformation and foreign-state coordinated inauthentic behaviour.
- 8.96 One of the stated barriers to greater threat intelligence sharing is the limited number of security-vetted staff working for social media platforms. Noting that there are some platforms with which it would be inappropriate to share any classified material, providing a greater degree of threat intelligence with appropriately vetted staff at trusted platforms would assist those platforms in streamlining efforts to counter foreign interference through social media.

Recommendation 12

- 8.97 The committee recommends the Australian Government establish a program of vetting appropriate personnel in trusted social media platforms with relevant clearances to ensure there is a point of contact who can receive threat intelligence briefings.**

³² Mr David Robinson, Director, Internet 2.0, *Committee Hansard*, 20 April 2023, p. 31

³³ Department of Industry, Science and Resources, *Safe and responsible AI in Australia: Discussion Paper*, June 2023, p. 4.

Building the capacity of civil society

- 8.98 The committee heard that Australians lack the information, expertise and resources to understand the risks presented by the use social media platforms and the information they engage with online.
- 8.99 Given the declining trust in democratic institutions and leaders, the increasing polarisation of opinion in society and the dominant role of social media platforms in our contested information environment, it is clear from the evidence received over the course of this inquiry that a coordinated national approach is required. While government and industry have a significant role to play, efforts to counter foreign interference and CIB through social media must include civil society.
- 8.100 The ability of civil society—individuals, organisations and community groups—to make informed decisions about information consumption and sharing needs to be expanded. To address the threat of foreign interference through social media, government support and funding is required to build this capacity.

Improving independent research and frameworks

- 8.101 The committee considered evidence supporting the role of expert centres and researchers—whether engaged by platforms or operating independently in civil society—to scrutinise the conduct of the platforms and those who seek to manipulate them for their own ends. These independent experts help people understand how social media platforms use and distribute data and content that is capable of shifting public opinion, including through personal data collection and use of algorithms which promote and filter content. Independent experts can also help highlight where these algorithms are being used maliciously or in an inauthentic manner to covertly sway public opinion or create chaos.
- 8.102 However, the committee is very aware that the effectiveness of independent research will be largely determined by the transparency of social media platforms as discussed in Recommendations 1 and 2—including in relation to their data collection policies, algorithms, and open access to social media platforms.
- 8.103 When provided access to relevant data, the committee has heard that expert centres and researchers can play a vital role in understanding how social media platforms operate, the effectiveness of foreign actors' content operations, and the nature and scale of certain cybersecurity threats.³⁴ Support from the Australian Government would ensure that cyber-enabled foreign interference

³⁴ See, for example: Department of Home Affairs, *Submission 1*, p. 3; University of Adelaide, *Submission 3*; US Federal Communications Commission, *Submission 4*, p. 2; RAND Australia, *Submission 11*, p. 3.

activities or campaigns in Australia could be more consistently and capably monitored and publicly reported.³⁵

- 8.104 This support could take the form of grant funding for social media monitoring and investigations, bolstering laws ensuring researchers can access more and higher-quality information data.³⁶
- 8.105 The committee also acknowledges the vital work that independent organisations undertake in exposing and analysing foreign interference. Expert Mr David Robinson told the committee that, in one instance, social media companies investigating commentary on their platforms after a particular event declared them to be free of interference. However, when using a mathematical analysis, Mr Robinson and other cybersecurity experts identified an interference campaign.³⁷
- 8.106 This example demonstrates that even when looking closely, sometimes even the platforms themselves cannot discern bots from people or campaigns of influence from genuine free expression. It requires the expertise of specialist organisations to review available data so that all of society can map an accurate picture of foreign interference. Some companies are more transparent than others when it comes to making data available for this kind of review due to commercial incentives, risk avoidance or other reasons. As such, Recommendations 1 and 2 will complement research efforts by ensuring platforms open themselves to independent cyber analysts and researchers to examine cyber-enabled foreign interference activities, but the Australian Government also needs to ensure independent researchers are supported to make the most of the opportunities this data provides.

Recommendation 13

- 8.107 The committee recommends the Australian Government build capacity to counter social media interference campaigns by supporting independent research.**

Protecting the public and diaspora communities

- 8.108 As technology continues to evolve, it is important that all elements of Australian society—government, business, civil society, and individuals—be equipped to respond appropriately to the threat of foreign interference and disinformation.
- 8.109 In addition to the recommendations above aimed at improving the integrity and transparency of all social media platforms operating in Australia, it is vital that the Australian Government lead an integrated whole-of-nation approach.

³⁵ CyberCX, *Submission 16*, p. 9.

³⁶ ASPI, *Submission 13*, p. 13.

³⁷ Mr David Robinson, *Internet 2.0, Committee Hansard*, 20 April 2023, p. 36.

This should include building the resilience of Australians, and particularly diaspora communities that might be subject to transnational repression and foreign interference. This can be achieved by building digital information and media awareness.

8.110 ASPI has identified that well-resourced state and non-state actors are misusing all forms of social media to 'facilitate the transnational repression of individuals and marginalised communities in Australia', which is of grave concern for our liberal democracy.³⁸

8.111 Over the course of this inquiry the committee heard compelling accounts diaspora communities and organisations on this rising trend of transnational repression. The perspectives of these community groups are uniquely important to the committee, as we understand they are often the targets of attempted foreign interference and victims of transnational surveillance, repression and coercion.

8.112 The committee heard powerful testimony from individuals personally targeted by foreign interference activities, and these experiences were instructive in contemplating how to address these threats.

8.113 Ms Vicky Xu, a journalist and policy analyst who was written extensively on the human rights abuses of the CCP told the committee:

I'm still dealing with death threats. I'm still dealing with repeated hacking attempts. Just this week I received a dozen hacking attempts across all of my accounts ... I've had to adapt the way I live, my lifestyle, to one that's akin to a criminal, I would say. People in democracies, politicians, academics and people with good social standing tell me things like I'm going to end up in history books, and that all sounds grand, but what about life?³⁹

8.114 Similarly, Badiucac told this committee:

... there are always certain topics that you cannot talk about. What happens is you'll be disappeared or your accounts will be suspended. This is actually a typical way of how the Chinese government manages to export its censorship outside of China regardless of local law or rights protection in Australian society. This is totally contradictory with our values, but functionally for Chinese diaspora and other people who are using WeChat, we actually have to be subject to China's law, which is not really a law for society. This for me is very unfair and fundamentally dangerous to our national security and core values of society.⁴⁰

8.115 In relation to an Iranian-Australian woman who has been outspoken on the human rights situation in Iran and advocated for the Iranian women's rights

³⁸ Australian Strategic Policy Institute, *Submission 13*, p. 3.

³⁹ Ms Vicky Xu, Senior Fellow, Australian Strategic Policy Institute, *Committee Hansard*, 21 April 2023, p. 35.

⁴⁰ Badiucac, Private capacity, *Committee Hansard*, 21 April 2023, p. 35.

movement, Mr Peter Murphy from the Australian Supporters of Democracy in Iran, said '[t]he basis of our democratic society include freedom of association, freedom of speech and freedom of expression, and this family in Melbourne has been told to stop talking, stop attending certain meetings and stop expressing certain views. It is really a blatant attack on our basic rights by a foreign government'.⁴¹

8.116 Additionally, Mrs Kateryna Argyrou from the Australian Federation of Ukrainian Organisations described how the Ukrainian-Australia diaspora is dealing with instances of harassment and intimidation:

We have tried to be very structured and systemised in the way that we approach it. Every time we've had a community member who has been harassed online or threatened – and we've had many community members who've received death threats through Telegram channels, through Facebook Messenger and through other social media – we've reported that to the police...we'd had over 40 official complaints registered with police.⁴²

8.117 The impact on individuals who have to live with this fear cannot be overstated. Many have fled authoritarian regimes and have chosen to live in Australia because of our rule of law and systems of democracy that protect our people from repressive tactics designed to silence dissent. Yet these same authoritarian states are misappropriating social media channels to reach into our nation to continue attempts to silence people through fear and intimidation. Liberal democracies like Australia must be resolute that we will not tolerate this behaviour and it must end now.

8.118 Law enforcement agencies and bodies such as the eSafety Commissioner are often privy to these personal experiences of coercion and repression, and as such are well-placed to share their observations and lessons learned with social media platforms and the broader public.

8.119 With the benefit of this knowledge, individuals and organisations will be better placed to make informed choices about their own online activities and identify and respond to foreign interference attempts they may be subject to in the future.

Recommendation 14

8.120 The committee recommends the Australian Government ensure that law enforcement agencies, and other relevant bodies such as the eSafety Commissioner, work with social media platforms to increase public awareness of transnational repression.

⁴¹ Mr Peter Murphy, Co-Secretary, Australian Supporters of Democracy in Iran, *Committee Hansard*, 21 April 2023, p. 22.

⁴² Mrs Kateryna Argyrou, Co-Chair, Australian Federation of Ukrainian Organisations, *Committee Hansard*, 21 April 2023, p. 28.

Improving digital and information literacy

- 8.121 One of the most effective buffers against foreign interference through social media is an informed, resilient population that is capable of identifying problematic content on their online feeds. It is vital that an integrated approach include supporting and building the resilience of Australians, particularly diaspora communities, through improved digital literacy and media awareness.
- 8.122 As technology continues to evolve, all Australians must be equipped to understand whether the information they are consuming is true or false, whether it comes from an authoritative source, whether it is emotionally manipulative, and whether they are presented with information from a diversity of sources.
- 8.123 The Australian Government should take steps to build resilience against foreign interference at the individual and community level by providing resources to better equip these groups to navigate the fraught digital information landscape. Efforts should prioritise at-risk communities, and should consider tailored messaging to address the specific needs of these groups.

Recommendation 15

- 8.124 The committee recommends the Australian Government empower citizens and organisations to make informed, risk-based decisions about their own social media use by publishing plain-language education and guidance material and regular reports and risk advisories on commonly used social media platforms, ensuring this material is accessible for non-English speaking citizens. Specific focus should be on protecting communities and local groups which are common targets of foreign interference and provide pre-emptive information and resources.**

Independent media

- 8.125 The committee has been reminded of the role of news media in providing reliable, accurate and apolitical news about politics and current events. It has received evidence about the potential dangers associated with consuming news content through social media, and the dangers of accessing information in an 'echo chamber' where people only encounter information or opinions which reflect and reinforce their own worldviews because of algorithmic preferences.
- 8.126 Furthermore, evidence heard by the committee shows authoritarian states control news and other content on some social media platforms used by Australians. For example, ASPI cited leaked content moderation documents which revealed that TikTok previously instructed its moderators to censor videos that mention Tiananmen Square, Tibetan independence, or the banned religious group Falun Gong.⁴³ This demonstrates the ways in which information

⁴³ Mr Fergus Ryan, Australian Strategic Policy Institute, *Committee Hansard*, 20 April 2023, p. 18–19.

can be filtered and manipulated to support the strategic interests of the interfering country, often in ways inimical to our own interests.

- 8.127 The committee heard of the specific challenges posed by TikTok and WeChat, given their ownership structures and the operation of Chinese national security laws. It also heard evidence of surveillance and restrictions of freedom of expression of Iranian- and Ukrainian-heritage people in Australia.
- 8.128 However, the committee also heard that independent reporting in the original languages of diaspora communities in Australia could play a key role in countering disinformation, content moderation, propaganda, censorship, and foreign influence through social media.
- 8.129 Witnesses explained that independent journalism provides diaspora communities with neutral and reliable sources of news about politics and current events. As noted by legal expert submitters, 'news and journalism generate significant benefits for society through the "production and dissemination of knowledge, the exposure of corruption, and holding Governments and other decision-makers to account"'.⁴⁴

Recommendation 16

- 8.130 **The committee recommends the Australian Government support independent and professional foreign-language journalism by supporting journalism training and similar programs, thereby expanding the sources of uncensored news for diaspora communities to learn about issues such as human rights abuses inside their country of origin.**

Protecting our neighbours

- 8.131 Australia has a strong, longstanding relationship with its Pacific neighbours. Australia's security cooperation with Pacific countries covers defence, law enforcement, transnational crime, climate and disaster resilience, border management and human security.
- 8.132 While the Australian Government is working with our Pacific neighbours through the Cyber and Critical Technology Cooperation Program to increase information technology resilience of governments and civil society we need to do more to specifically address the impacts that foreign interference can have both on governments and ordinary people across our neighbouring regions.
- 8.133 The Australian Government should consider ways to extend the learnings and benefits of the other initiatives recommended by this report to our regional neighbours. These efforts will build country-to-country linkages, and empower our neighbours to identify and thwart foreign interference attempts within their own communities.

⁴⁴ The Law Society of New South Wales Young Lawyers, *Submission 33*, p. 17.

Recommendation 17

8.134 The committee recommends the Australian Government promote the digital literacy and the infrastructure of developing countries in the Indo-Pacific region that are the targets of malicious information operations by foreign authoritarian states.

**Senator James Paterson
Chair
Liberal Senator for Victoria**

Additional comments from Government Senators

- 1.1 We thank the committee Chair, Senator Paterson, and committee members for conducting a comprehensive inquiry on a matter of national significance in a collegiate spirit.
- 1.2 The risk of foreign interference is real across all social media platforms.
- 1.3 Misinformation and disinformation, coordinated inauthentic behaviour (CIB) and foreign interference through social media pose a threat to Australia's social cohesion, national security and to the ability of diaspora communities to participate fully and without fear in our democracy.
- 1.4 Platforms must take greater responsibility for combating these harmful practices.
- 1.5 While evidence from platforms indicated they have some measures in place, there are significant differences and gaps in platform practices and reporting. Overall, platform transparency measures are insufficient and inconsistent, particularly when it comes to specific reporting on the Australian context.
- 1.6 The committee has recommended a minimum set of transparency requirements, enforceable with fines. Government Senators welcome the committee's core focus on transparency measures.
- 1.7 In January 2023, the Minister for Communications announced that the Australian Government would introduce new laws to provide the independent regulator, the Australian Communications and Media Authority (ACMA), with new powers to combat online misinformation and disinformation.
- 1.8 The new powers will enable the ACMA to require platforms to address misinformation and disinformation, while balancing freedom of speech.
- 1.9 The proposed powers mirror those proposed by the committee, and will enable the ACMA to gather information from platforms and require them to keep records about misinformation and disinformation.
- 1.10 Evidence to this inquiry has further highlighted the urgent need for powers like these, to ensure consistent, transparent, Australia-focussed information is available from platforms to inform users.
- 1.11 The proposed legislation also gives the ACMA the power to enforce an industry-led code of practice covering measures to combat misinformation and disinformation, and to create and enforce a new industry standard, if required.
- 1.12 The committee has proposed a list of specific requirements that could be considered as part of such a new code, including requiring social media platforms to have an Australian presence to ensure accountability to the Parliament and people, labelling state-affiliated media, disclosing instances of

transnational repression, and greater transparency about levels of CIB and takedowns of networks and materials. We commend the list of measures in Recommendation One for further consideration by the Australian Government.

- 1.13 Blunt, national bans of specific platforms as a policy approach were not supported by evidence to the committee.
- 1.14 One submitter described single platform bans as a 'whack-a-mole approach', given the relative ease with which platforms could take data and reestablish, and the frequency with which new platforms emerge in the global market. Others raised concerns about whether bans can be practically implemented, and the implications for users on these platforms.
- 1.15 For these reasons, the committee's central focus is on strong regulation for transparency, rather than nation-wide bans of specific platforms.
- 1.16 In relation to bans on government devices, the Australian Government has taken an appropriate and targeted approach, by seeking advice from intelligence and security agencies and issuing a mandatory direction under the Protective Security Policy Framework to prohibit TikTok on devices issued by Australian Government departments and agencies.
- 1.17 We note that any further approaches to bans or policies for government or government-related devices should similarly be informed by advice from agencies.
- 1.18 The committee notes that a whole-of-government approach is required to combat foreign interference through social media. Departments and agencies including Home Affairs, the Australian Federal Police, Australian Electoral Commission, the eSafety Commissioner and intelligence agencies gave evidence of their collaboration today to protect Australians. Home Affairs, as the lead department in countering foreign interference, outlined the central role of the Counter Foreign Interference Coordination Centre (CFICC) within Home Affairs in leading multi-department and agency collaboration.
- 1.19 One of the most concerning themes in evidence was instances of harassment of Australian citizens within diaspora communities as they exercise their democratic rights to speak out on matters pertaining to their country of origin. This whole-of-government approach is needed to protect at-risk communities. Work to continually improve the resources of, and responses to, diaspora communities is critical. The committee recommends supporting diverse, independent foreign-language journalism in Australia, as part of this approach.
- 1.20 We note that the committee has provided a range of further thoughtful recommendations for the consideration of the Australian Government, including in the areas of the security implications of artificial intelligence (AI), supporting independent research, and further assisting our Pacific neighbours to combat foreign interference in the region.

- 1.21 Once more, we thank the Chair, committee members, submitters and witnesses and the Secretariat for their considered work on a topic of critical importance to our nation.

Senator Jess Walsh
Deputy Chair
Labor Senator for Victoria

Senator Raff Ciccone
Member
Labor Senator for Victoria

Australian Greens' Additional Comments

- 1.1 The Greens welcome the committee's recommendations for a minimum set of transparency requirements which social media companies must comply with and which are enforceable with fines.
- 1.2 The recommendations fail to further include data minimisation requirements which protect the sensitive data of users and their digital rights.
- 1.3 The Greens do not support platform-specific reforms because this fails to tackle the core of the issue. We urgently need a platform-neutral approach to policy because targeting a single platform based on the country it is linked to does nothing to protect Australians from foreign interference.
- 1.4 Banning TikTok or any other singular platform from government devices is nothing but a game of digital whack-a-mole and does nothing to protect Australians. Bad actors will use their vast resources through whatever means necessary to meet their objectives and until we address the underlying causes Australians will continue to be subject to foreign interference threats.

Senator Sarah Hanson-Young
Member
Greens Senator for South Australia

Senator David Shoebridge
Member
Greens Senator for New South Wales

Appendix 1

Submissions, tabled documents and additional information

- 1 Department of Home Affairs
- 2 Australian Security Intelligence Organisation
- 3 University of Adelaide, Defence Security Institute
- 4 U.S. Federal Communications Commission
- 5 Australian Signals Directorate
- 6 Australian Communications and Media Authority
- 7 Department of Infrastructure, Transport, Regional Development,
Communications and the Arts
- 8 Australian Electoral Commission
- 9 Australian Human Rights Commission
- 10 eSafety Commissioner
 - 10.1 Supplementary to submission 10
 - Attachment 1
- 11 RAND Australia
- 12 Human Rights Watch
- 13 Australian Strategic Policy Institute
- 14 SBS
- 15 WeChat
- 16 CyberCX
- 17 Internet 2.0
 - Attachment 1
- 18 Dr William Stoltz
- 19 Allens Hub joint submission (UNSW Allens Hub; Deakin CSRI; IEEE SSIT)
- 20 Ms Sarah Kendall
- 21 News & Media Research Centre
- 22 Dr Samuel White
- 23 Australian Supporters of Democracy in Iran
 - 23.1 Supplementary to submission 23
- 24 Australian Muslim Advocacy Network
- 25 Attorney-General's Department
- 26 Reset Australia
- 27 Law Council of Australia
- 28 University of Melbourne, UNSW, University of Adelaide
- 29 Internet Governance Project, Georgia Tech
 - Attachment 1

- 30 TikTok Australia
- 31 Australian Tibetan Communities Association
- 32 Meta Australia
- 33 NSW Young Lawyers
- 34 Rachel Lee, Prudence Luttrell, Matthew Johnson, John Garnaut
- 35 Digi Industry Group Inc
- 36 Simon Jiandan
- 37 Professors Wanning Sun & Haiqing Yu
- 38 Confidential
- 39 Ms Vanessa Teague
- 40 Confidential

Tabled Documents

- 1 Document tabled by Senator David Van at a public hearing in Canberra, 21 April 2023.
- 2 Document tabled by Senator James Paterson at a public hearing in Canberra, 12 July 2023.

Answer to Question on Notice

- 1 LinkedIn, answers to questions on notice, 11 July 2023 (received 14 July 2023)
- 2 ACMA, answer to questions on notice No. 1, 12 July 2023 (received 14 July 2023)
- 3 ACMA, answer to questions on notice No. 2, 12 July 2023 (received 14 July 2023)
- 4 ACMA, answer to questions on notice No. 3, 12 July 2023 (received 14 July 2023)
- 5 ACMA, answer to questions on notice No. 4, 12 July 2023 (received 14 July 2023)
- 6 ACMA, answer to questions on notice No. 5, 12 July 2023 (received 14 July 2023)
- 7 ACMA, answer to questions on notice No. 6, 12 July 2023 (received 14 July 2023)
- 8 Attorney-General's Department, answer to questions on notice, 12 July 2023 (received 17 July 2023)
- 9 TikTok Australia, answers to questions on notice (1, 9, 10) 11 July 2023 (received 14 July 2023)
- 10 TikTok Australia, answers to written questions on notice (5) 11 July 2023 (received 17 July 2023)
- 11 Department of Home Affairs, answers to questions on notice (no. 1) 12 July 2023 (received 18 July 2023)
- 12 Department of Home Affairs, answers to questions on notice (no. 2) 12 July 2023 (received 18 July 2023)
- 13 Department of Home Affairs, answers to questions on notice (no. 3) 12 July 2023 (received 18 July 2023)

-
- 14 Department of Home Affairs, answers to questions on notice (no. 4) 12 July 2023 (received 18 July 2023)
 - 15 Department of Home Affairs, answers to questions on notice (no. 5) 12 July 2023 (received 18 July 2023)
 - 16 Department of Home Affairs, answers to questions on notice (no. 6) 12 July 2023 (received 18 July 2023)
 - 17 Department of Home Affairs, answers to questions on notice (no. 7) 12 July 2023 (received 18 July 2023)
 - 18 TikTok Australia, answers to written questions on notice (2, 3, 4) 11 July 2023 (received 19 July 2023)
 - 19 TikTok Australia, answers to questions on notice (2, 3, 7, 8) 11 July 2023 (received 19 July 2023)
 - 20 Australian Electoral Commission, answer to question on notice, IQ23-000002, 12 July 2023 (received 19 July 2023)
 - 21 Meta Australia, answers to questions on notice (1-9) 11 July 2023 (received 19 July 2023)
 - 22 Meta Australia, answers to written questions on notice (1-11) 11 July 2023 (received 19 July 2023)
 - 23 TikTok Australia, answers to questions on notice (4, 5, 6), 11 July 2023 (received 21 July 2023)
 - 24 TikTok Australia, answers to written questions on notice (1), 11 July 2023 (received 21 July 2023)
 - 25 Twitter, answers to questions on notice, 11 July 2023 (received 25 July 2023)
 - 26 Twitter, answers to questions on notice, 11 July 2023 (received 25 July 2023)
 - 27 We Chat, answers to written questions on notice, 17 July 2023 (received 26 July 2023)
 - 28 TikTok, answers to questions on notice (6) 11 July 2023 (received 26 July 2023)
 - 29 TikTok Australia, answers to questions on notice (7 annexure) 11 July 2023 (received 19 July 2023)

Appendix 2

Public hearings and witnesses

Thursday, 20 April 2023

Committee Room 2S3

Parliament House

Canberra

Ms Shanthi Kalathil (via videoconference), Private capacity

U.S. Federal Communications Commission (via videoconference)

- Commissioner Brendan Carr, Commissioner

Dr Seth Kaplan (via videoconference), Private capacity

Australian Strategic Policy Institute

- Mr Fergus Ryan, Senior Analyst
- Mr Albert Zhang, Analyst
- Ms Emily Mosley, International Cyber Policy Centre Coordinator

RAND Australia

- Dr Andrew Dowse, Director

Internet 2.0 (via videoconference)

- Mr David Robinson, Director

Dr William Stoltz (via videoconference), Private capacity

Professor Rory Cormac (via videoconference), Private capacity

Friday, 21 April 2023

Committee Room 2S3

Parliament House

Canberra

Human Rights Watch

- Ms Elaine Pearson, Asia Director
- Ms Yaqiu Wang, Senior China Researcher (via videoconference)

Alliance for Securing Democracy

- Ms Lindsay Gorman, Senior Fellow and Head of the Technology and Geopolitics Team (via videoconference)

Mr Kenny Chiu (via videoconference), Private capacity

Australian Supporters of Democracy in Iran

- Mr Peter Murphy, Co-Secretary

Australian Tibetan Communities Association

- Mr Kalsang Tsering, President (via videoconference)

Australian Federation of Ukrainian Organisations

- Mrs Kateryna Argyrou, Co-Chair

Vicky Xu (via videoconference), Private capacity

Badiucio (via videoconference), Private capacity

Tuesday, 11 July 2023

Main Committee Room

Parliament House

Canberra

Meta Australia

- Mr Josh Machin, Head of Public Policy, Australia

Meta Australia

- Ms Mia Garlick, Director of Policy Australia and New Zealand

LinkedIn

- Mr Joshua Reiten, Senior Director, Digital Safety

TikTok Australia

- Ms Ella Woods-Joyce, Director of Public Policy

TikTok Australia

- Mr Will Farrell, US Data Security

TikTok Australia

- Mr Lee Hunter, General Manager, Australia

Google

- Mr Shane Huntley, Senior Director and Global Lead, Google Threat Analysis Group

You Tube Australia

- Ms Rachel Lord, Senior Manager, Public Policy and Government Relations

Twitter

- Ms Kathleen Reen, Senior Director of Public Policy, JAPAC

Twitter

- Mr Nick Pickles, Head of Global Government Affairs

Wednesday, 12 July 2023

Main Committee Room

Parliament House

Canberra

Department of Home Affairs

- Ms Sally Pfeiffer, A/g FAS Counter Foreign Interference
- Mr Peter Anstee, A/g FAS Digital Security Policy

Australian Security Intelligence Organisation

- Mr Mike Noyes, Deputy Director-General, Intelligence Service Delivery

Australian Signals Directorate

- Ms Abigail Bradshaw, Acting Director-General
- Ms Stephanie Crowe, Acting Head Australian Cyber Security Centre
- Mr Daniel Tripovich, Assistant Director-General Standards, Technical Advice and Research

Attorney-General's Department

- Mr Parker Reeve, Assistant Secretary: Transparency and Administration Law
- Ms Catherine Fitch, A/g First Assistant Secretary, Integrity Frameworks Division
- Ms Sarah Chidgey, Deputy Secretary, National Security and Criminal Justice

Australian Federal Police

- Mr Christopher Goldsmid, Commander Cybercrime Operations, Cyber Command
- Mr Stephen Nutt, Commander Special Investigations, Counter Terrorism and Special Investigations Command

Australian Communications and Media Authority

- Ms Cathy Rainsford, General Manager, Content & Consumer Division
- Ms Nerida O'Loughlin, Chair

Office of the eSafety Commissioner

- Mr Toby Dagg, Acting eSafety Commissioner

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

- Mr Sam Kursar, Director, Information Integrity Section
- Mr Andrew Irwin, Acting Assistant Secretary, Platforms and News Branch
- Mr Richard Windeyer, Deputy Secretary, Communications and Media Group

Australian Electoral Commission

- Mr Tom Rogers, Electoral Commissioner
- Mr Jeff Pope, Deputy Electoral Commissioner

Appendix 3

46th Parliament inquiry recommendations

Recommendations from interim report of 46th Parliament

- 1.1 The following section details the recommendations made by the Select Committee on Foreign Interference through Social Media in the 46th Parliament, and any progress on those recommendations as at February 2023.

Recommendation 1

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

- 1.2 Lead accountability continues to be shared across Government, including by the Department of Home Affairs, the Australian Security and Intelligence Organisation (ASIO), and the Australian Federal Police (AFP), with the Counter Foreign Interference Taskforce sitting within Home Affairs. However, it is also evident that there remain a number of key departments in this space, including also the Attorney-General's Department (including the National Security Hotline), the Department of Foreign Affairs and Trade (DFAT) and Department of Finance, as well as agencies including the Australian Electoral Commission (AEC), the Australian Communications and Media Authority (ACMA), and the Australian Competition and Consumer Commission (ACCC).¹

Recommendation 2

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.

- 1.3 On 14 February 2023, the Minister for Home Affairs announced a new community outreach program to be coordinated by Home Affairs and ASIO. The program will identify individuals within the Australian community who might be targets of foreign interference and design and deliver a program to proactively help them understand what foreign interference is, how they can respond, and what the Government can do to protect them. This is in addition to the existing Home Affairs counter interference engagement officers in each

¹ ACMA, [Release of ACMA's disinformation report](#), 21 March 2022; Australian Competition and Consumer Commission, [ACCC September 2022 Digital Platform Services Inquiry Report on Regulatory Reform – Key Findings](#), [2022].

state and territory, who work with a 'network of people who we believe might be targeted in engagements of foreign interference'.²

- 1.4 On 27 February 2023, the AFP announced the launch of an education campaign to help culturally and linguistically diverse communities (CALD) understand what FI is, how it manifests itself and where victims can report instances and seek assistance. It will include a factsheet, translated into more than 30 languages and meetings between AFP community liaison teams and CALD groups and religious leaders.³

Recommendation 3

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.

- 1.5 Established in 2019, the role of the Electoral Integrity Assurance Taskforce is to safeguard Australia's electoral integrity. The Taskforce provides a mechanism for sharing and referring relevant information (including foreign interference material) between relevant agencies.⁴
- 1.6 The AEC is aware of the threat to democracy of mis and disinformation, including through social media, and in 2021 released a Reputational Management Strategy and complementary Disinformation Register (for current election events).⁵
- 1.7 Guidance on caretaker conventions were updated in December 2021 and currently contain no specific guidance on classified briefings for the Opposition during the caretaker period with respect to foreign interference, noting that the ASIO Act already makes provision for the Leader of the Opposition to be

² The Hon Clare O'Neil MP, Minister for Home Affairs, *Foreign interference in Australia — ANU address*, 14 February 2023, [p. 5].

³ Australian Federal Police, '[AFP launches new resource to help combat foreign interference](#)', *Media release*, 27 February 2023, (accessed 27 February 2023).

⁴ Electoral Integrity Assurance Taskforce, [Australian Electoral Commission, Foreign interference \[factsheet\]](#). See also: Australian National Security, Report suspicious behaviour, www.nationalsecurity.gov.au/what-can-i-do/report-suspicious-behaviour (accessed 15 February 2023); Department of Home Affairs, *Countering foreign interference*, www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference (accessed 15 February 2023).

⁵ Australian Electoral Commission, [Electoral integrity: Reputation Management Strategy](#), 2021, pp. 3–4; Australian Electoral Commission, *Disinformation register*, <https://aec.gov.au/media/disinformation-register.htm> (accessed 15 February 2023).

'consulted regularly ... for the purpose of keeping him or her informed on matters relating to security'.⁶

Recommendation 4

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.

- 1.8 The report was completed in June 2021 and released on 21 March 2022.⁷
- 1.9 Annual transparency reports about the functioning of The Australian Code of Practice on Misinformation and Disinformation (DIGI code) are also published by Digital Industry Group Inc (DIGI).⁸
- 1.10 In December 2022, DIGI strengthened the code, making changes in response to stakeholder feedback received through a planned review of the code. Changes included an improved definition of 'harm' in relation to mis and disinformation and additional commitments reflecting updates to the strengthened European Union Code of Practice. DIGI also introduced more proportionate annual transparency reporting requirements for smaller platforms to encourage them to adopt the code, which can be flexibly applied to different types of digital service providers.
- 1.11 These updates are the latest set in a series of improvements driven by DIGI and code signatories since the DIGI code was introduced in February 2021. In October 2021, DIGI introduced independent oversight and a complaints facility to increase accountability. In 2022, independent assessment and best practice reporting guidelines were introduced to drive improvements in the transparency reporting process.⁹

Recommendation 5

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

⁶ Australian Security Intelligence Organisation Act 1979, s. 21.

⁷ Australian Communications and Media Authority, [Report to government on the adequacy of digital platforms' disinformation and news quality measures](#), June 2021; Australian Communications and Media Authority, [Release of ACMA's disinformation report](#), 21 March 2022, www.acma.gov.au/articles/2022-03/release-acmas-disinformation-report (accessed 23 February 2023).

⁸ DIGI, *Transparency reports*, <https://digi.org.au/disinformation-code/transparency/> (accessed 15 February 2023).

⁹ DIGI, *DIGI Welcomes The Government Providing ACMA With Oversight Powers Over Misinformation*, 20 January 2023, <https://digi.org.au/digi-welcomes-the-government-providing-acma-with-oversight-powers-over-misinformation/> (accessed 23 February 2023).

1.12 The terms of reference were published 27 October 2022.¹⁰

Recommendation 6

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.

1.13 The nature of arrangements, including reporting arrangements, with social media platforms are not publicly available.

1.14 As part of the DIGI code signatories, including social media platforms, commit to identify and address mis and disinformation:

As part of this [Complaints] process, Signatories will also consider how they can leverage current arrangements with government and relevant regulatory agencies to identify and address instances of Inauthentic Behaviours that propagate Disinformation and are the subject of measures addressed by this Code.¹¹

1.15 Following the release of its June 2021 report, the ACMA anticipated that the Government would establish the Misinformation and Disinformation Action Group (MADAG) to support collaboration and information-sharing between key stakeholders on issues relating to disinformation and misinformation.¹²

Recommendation 7

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.

1.16 In general terms, under the Taskforce's terms of reference it is responsible for 'assessing and understanding the vulnerability of Australia's federal electoral environment, and developing strategies and processes to ensure cohesive and effective management and response should any threats be realised'.¹³

1.17 Public information about the Taskforce's work is limited.

¹⁰ Australian Electoral Commission, [Electoral Integrity Assurance Taskforce: terms of reference](#), 27 October 2022.

¹¹ DIGI, [Australian code of practice on disinformation and misinformation](#), Updated 22 December 2022, p. 21.

¹² Department of Infrastructure, Transport, Regional Development, Communications and the Arts, [Media release: New disinformation laws](#), 21 March 2022.

¹³ Australian Electoral Commission, *Electoral Integrity Assurance Taskforce: terms of reference*, 27 October 2022, p. 1.