Australian Human Rights Commission

# Inquiry into the risk posed to Australia's democracy by foreign interference through social media

Australian Human Rights Commission

Submission to Senate Select Committee on Foreign Interference through Social Media

16 February 2023

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
Complaints info line 1300 656 419
TTY 1800 620 241

Australian Human Rights Commission
www.humanrights.gov.au

## Contents

# 1 Introduction

1. The Australian Human Rights Commission (the Commission) welcomes the opportunity to make this submission to the Senate Select Committee on Foreign Interference through Social Media (the Inquiry).
2. The role of the Commission is to work towards an Australia in which human rights are respected, protected and promoted. While the Commission has expertise and knowledge in the area of human rights generally, relevant to this Inquiry it has also developed specific expertise with respect to the human rights risks posed by new and emerging technologies. Most recently, this can be seen in the Human Rights and Technology Project, which was a three-year, national investigation that culminated with the release of the Human Rights and Technology Project Final Report in 2021.
3. The use of social media by foreign actors to improperly interfere in global events has become a significant concern in recent times. With the proliferation of social media platforms, and the ease with which information spreads online, foreign entities now possess an unprecedented ability to interfere with the information received by all Australians, which in turn has significant implications for human rights within Australia more generally.
4. From the outset, it is important to recognise the paradox that lies at the heart of this issue, namely that social media can be used for purposes that both strengthen *or* undermine Australia's democracy and values. On the one hand, social media can be used in ways that increase access to information and opportunities for the free exchange of ideas, increase the diversity of voices contributing to public discussions and allow for broader public participation in our democracy. On the other hand, social media can also be used in ways that pose a threat to democratic processes through social medial campaigns that spread misinformation and disinformation, undermine trust in public institutions and exacerbate divisions within society. The challenge lies in ensuring that any policy responses mitigate the risks posed by the latter, without disproportionately impacting upon the former.
5. Governments and social media companies have sought to prevent foreign interference through social media using a range of policy responses, including increased scrutiny of online activity during elections, the implementation of rules and policies to prevent the spread of misinformation and disinformation and the use of advanced algorithms to detect and remove fake accounts and other forms of interference.

However, the Commission considers there is more Australia should be doing in response, particularly considering the growing number, and sophistication, of foreign interference operations online.

# 2 Definitions

6. The Terms of Reference for this Inquiry specifically refer to both misinformation and disinformation. Throughout this submission we have adopted the same definitions for these terms as provided by the Electoral Integrity Assurance Taskforce, namely:[1]
   - 'Misinformation' is false information that is spread due to ignorance, or by error or mistake, without the intent to deceive.
   - 'Disinformation' is knowingly false information designed to deliberately mislead and influence public opinion or obscure the truth for malicious or deceptive purposes.
7. The distinction between foreign interference and foreign influence was set out in the First Interim Report published by the Select Committee on Foreign Interference through Social Media appointed in the previous Parliament (First interim Report),[2] and also highlighted by the Electoral Integrity Assurance Taskforce.[3]
8. 'Foreign interference' concerns foreign powers seeking to secretly and improperly interfere in Australia's society to advance their strategic, political, military, social or economic goals, at the expense of Australia's own. 'Foreign influence' involves a government seeking to influence deliberations on issues of importance to them.
9. The Electoral Integrity Assurance Taskforce has emphasised that Australia is not concerned with foreign influence activity that is open and transparent, and that respects our people, society and systems.[4] This submission adopts that distinction, with the concerns raised below relating solely to instances of foreign interference.

# 3 Social media and human rights risks

10. 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 population) had active social media accounts, and that 52% of Australians use social media as a source of news.[5] While there are many positives to

these digital spaces, there are also latent risks associated with their pervasiveness.

11. Given the indispensable nature of social media in the modern world, foreign entities have correctly identified it as an effective and inexpensive environment through which to conduct interference operations aimed at unduly influencing geopolitics, achieving strategic objectives and potentially undermining democratic processes and human rights.[6] Unsurprisingly, foreign interference operations during elections and referendums have increased significantly in the online environment in recent years.[7]

12. The Commission is especially concerned about coordinated inauthentic behaviour (CIB). CIB generally refers to coordinated efforts to manipulate public debate for strategic reasons, where fake accounts are paramount to the endeavour.[8] CIB operations are already occurring in Australia[9] and instances of their use are likely to increase as time continues.

13. The risk posed by foreign interference through social media is a real and immediate concern. In their most recent Annual Report, the Australian Security Intelligence Organisation (ASIO) said that espionage and foreign interference have supplanted terrorism as Australia's principal security concerns. Cyberspace remains the 'most pervasive vector for espionage' and '[m]ultiple foreign governments are determined to interfere in Australia's democracy and undermine our sovereignty'.[10]

14. Foreign interference via social media is nuanced and evolving, which is why Australians (and the Australian Government) must remain vigilant and develop pro-active policy responses to protect our democracy. The Commission is increasingly concerned about the negative impact that foreign interference through social media can potentially have on democracy and human rights in Australia, highlighting three particular risks:

    - misinformation and disinformation;
    - risks to privacy; and
    - increasing censorship.

15. There are a range of individual human rights potentially impacted by the use of social media in this way, with key examples including the right to freedom of expression,[11] right to privacy,[12] and the right to take part in public affairs.[13]

## 3.1 Misinformation and disinformation

16. Social media has become a breeding ground for misinformation and disinformation – being an easily accessible and relatively inexpensive tool which can spread content rapidly across a large population. Both misinformation and disinformation can have devastating effects on human rights, social cohesion and democratic processes. Indeed, this can be the very purpose intended by the release of disinformation.

17. Disinformation is promoted by foreign actors (both state and non-state actors) to pursue their strategic interests and influence public opinion in Australia and abroad.[14]

18. It disseminates rapidly and inexpensively, which makes it a useful tool in online interference operations. The News and Media Research Centre identified three factors in particular which exacerbated the spread of disinformation:[15]

    - digital networks play a central role in political communication;
    - the speed at which disinformation transmits on social media renders information attacks difficult to counter; and
    - digital influence operations have low implementation costs.

19. Foreign interference operations utilising disinformation are also inadvertently assisted by how Australians consume news media. Often disinformation is posted as content which is promoted as 'fact' or 'news' on social media.

20. The Digital News Media Report: Australia 2022 highlights an overall downward trend in the use of social media as a source of news, which currently sits at 19% and is down four percentage points from last year.[16] However, for Generation Z (those born after 1997), 46% use social media as their main source of news (although this still represents an eight percentage point drop from last year).[17] This percentage is also higher for Generation Y (also known as 'Millennials' –born between 1981 and 1996), sitting at 28% – which represents a nine percentage point reduction in the past year.[18]

21. Although the consumption of news through social media has reduced since 2020,[19] there is still a high number of Australians – and particularly a high number of young Australians – who consume news through social media. These individuals are especially at risk of being influenced by foreign interference operations which present disinformation as 'news'.

22. The First Interim Report provided examples of CIB operations by foreign actors that attempted to spread disinformation online.[20] The Department of Home Affairs submitted that it regularly observes 'campaigns unfold on social media that involve disinformation'. For example, in 2017, accounts linked to a foreign government entity were involved in discussions related to a plot to bomb an Etihad airlines flight departing Sydney International Airport. One account used the disrupted plot to promote and amplify the hashtags #MuslimBan and #StopImportingIslam.[21] Both the quantity and quality of these types of disinformation campaigns can be expected to increase into the future, largely driven by continuing advances in the technology that is used, and the ease with which it can be deployed.

23. Social polarisation is often a goal for foreign actors on social media, as they pit groups against one another to further their own agendas.[22] This can often build upon, or amplify, existing tensions or divisions in a society. The Commission 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.

24. While social media platforms use a mixture of automated technology and human investigators to address misinformation and disinformation, the Commission considers current efforts to be inadequate. Social media platforms have struggled to effectively combat the growing volumes of misinformation and disinformation, which can lead to the marginalisation and persecution of certain groups.

25. 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.

26. There are a range of existing laws that apply to social media (including the *Online Safety Act 2021* (Cth)), as well as a range of other policy measures adopted by government and by social media platforms themselves. For example, with respect to misinformation and disinformation specifically, the second set of transparency reports under the Australian Code of Practice on Disinformation and Misinformation (Code) were published in May 2022,[23] and the Code itself was updated in December 2022. However, 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.

27. The broader question of misinformation and disinformation on social media is an important one that needs to be given serious consideration,

and invites a range of policy responses from both government and industry. The Terms of Reference of this Inquiry, however, focus specifically on the risk posed to Australia's democracy by foreign interference through social media. In addressing this specific risk to sovereignty, responsibility necessarily lies with the Australian government. Given the nature of the risk, improved industry safeguards or responses alone cannot be a sufficient response.

28. 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.

**Recommendation 1: The Australian Government should establish a permanent whole-of-government taskforce dedicated to preventing and combating foreign interference by way of cyber-manipulation in Australia.**

29. The Australian Government should also establish clear and mandatory requirements and pathways for social media organisations to report suspected foreign interference activities. Such reports should be made to the proposed whole-of-government taskforce outlined above in Recommendation 1.

30. While acknowledging that this taskforce may be dealing with sensitive and protected information, it should be required – to the extent reasonably possible – to report publicly on the reports received and activities undertaken. The aim should be 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.

31. 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.

32. The guidance provided by the UN Human Rights Committee in General Comment No. 34, with respect to the permissible limitations on the right to freedom of expression, is particularly relevant here:

> … when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself. The Committee recalls that the relation between right and restriction and between norm and exception must not be reversed.[24]

33. There are also dangers inherent in allowing any one body – be it government, a government taskforce, or a social media platform – to become the sole arbiter of 'truth'. There is a real risk that efforts to combat online misinformation and disinformation by foreign actors could be used to legitimise attempts to restrict public debate, censor unpopular opinions and enforce ideological conformity in Australia. All efforts to combat misinformation and disinformation need to be accompanied by transparency and scrutiny safeguards to ensure that any limitations imposed upon freedom of expression are no greater than absolutely necessary and are strictly justified.

34. There must also be a clear separation of issues of national interest and security from narratives that may result in demonisation or vilification of particular communities in Australia (such as Chinese communities, and those who are racialised as Chinese).

**Recommendation 2: The Australian Government should establish clear and mandatory requirements, and pathways, for social media organisations to report suspected foreign interference. Such reports should be made to the permanent taskforce noted above in Recommendation 1, whose activities in this area must incorporate robust safeguards to protect freedom of expression.**

35. The Australian public can also play an important role in countering foreign interference through social media. Increasing digital literacy throughout the general community would help to ensure that the Australian population are better able to recognise and respond appropriately to the risks of misinformation and disinformation online, which would increase national resilience in respect of these risks.

36. The starting point here is to ensure that there is greater investment in incorporating digital literacy into the Australian education curriculum. This should include information about online safety, data privacy, identifying misinformation and disinformation and the role that algorithms play in a users' online experience.

37. In addition to investment in the Australian curriculum, the Australian Government should introduce a public education campaign on digital literacy and develop online digital literacy resources that are available to the general public. The campaign and resources should include information and materials that enable Australians to better identify, and counter, misinformation and disinformation online. They should be tailored to different demographics and ensure accessibility for all Australians, with a particular focus on ensuring that the campaign and resources effectively engage with elderly people, people from culturally and linguistically diverse backgrounds, people from low-income backgrounds, people in regional and rural areas and people with disability. These should also be designed with caution in order to avoid vilifying any particular communities in Australia (such as Chinese communities).

**Recommendation 3: The Commonwealth and state and territory governments must increase their investment in incorporating digital literacy into the Australian curriculum, including information about online safety, data privacy, identifying misinformation and disinformation and the role algorithms play in a users' online experience.**

**Recommendation 4: The Australian Government should introduce a public education campaign on digital literacy and develop online digital literacy resources that are available to the general public.**

## 3.2 Risks to privacy

38. Social media platforms often collect vast amounts of personal data from their users, which can potentially be accessed and used by third parties without the individual user's knowledge or consent. This can lead to invasions of privacy and the potential abuse of personal information. The right to privacy is a human right recognised in numerous international human rights instruments and treaties.[25]

39. All people have a right to privacy, which has become increasingly relevant in the 21st century. While previously this protected people's personal lives

at home, it now must extend to their personal information and online lives. This is a right which is comprehensively discussed below and of increasing relevance in counter foreign interference operations.

40. The protection of the right to privacy is essential for people to live with dignity and security. Yet the vulnerability of personal information online provides an opportunity for foreign interference through the misuse of this personal data. Recent data breaches in Australia, including both the Optus and Medibank Private data breaches, have highlighted the increasing vulnerability of Australians to cyber-attacks, and the vital importance of cyber security.

41. The collection of personal data by social media platforms allows algorithms to tailor content to individual users. This personal information helps to create a user profile which allows social media companies to tailor the user experience to each individual, and also to sell targeted advertising.[26]

42. An unfortunate phenomenon with such targeted content is that users tend to be shown more, and gravitate towards, sensationalist clickbait[27] – which often forms the basis of foreign interference operations on social media. This is due to the primary aim of social media platforms being to maximise the time that users spend on their platform (which in turn increases advertising revenue potential). Accordingly, algorithms are incentivised to provide content which is meant to be more engaging for users. However, this material is often more extremist, sensationalist or plainly incorrect,[28] with algorithms having 'learnt' that such content garners greater engagement. It is by this process that foreign entities can introduce inflammatory material, which is then promoted by algorithms using microtargeted advertising, encouraging further user engagement and amplifying the reach of the content.[29] The algorithms appear to prioritise optimising user engagement and advertising revenue over the human rights and safety of users.

43. The highly tailored nature of microtargeted advertising has previously been used to interfere with democratic processes. A key example of this was the harvesting of some 87 million Facebook users' personal information by Cambridge Analytica, with that information being used for microtargeted targeted political advertising in the 2016 United States presidential election and 2016 Brexit campaign.[30]

44. The harvesting of personal data for advertising purposes has significant implications in terms of privacy and also the ability to amplify the existing phenomena known as 'echo chambers'. An echo chamber is an online environment where a person only encounters information, or opinions,

which reflect and reinforce their own worldviews.[31] These echo chambers can play a role, in conjunction with limited content moderation, in facilitating the spread of misinformation and disinformation, reinforcing hate speech and prejudicial content online and allowing for amplification of extremist views and conspiracy theories.

45. Only a minority of people truly understand the role that algorithms play in curating content shown to users on social media.[32] This can often make it difficult for users to escape online echo chambers, and highlights the need for greater education about how algorithms use personal data to tailor online experiences.[33]

46. The implementation of awareness campaigns, such as the Australian Electoral Commission's 'Stop and Consider' campaign in the lead-up to the 2019 Federal election, is a constructive example of how the Australian public can be taught to critically examine the content they see online.[34]

47. The digital literacy campaign and materials recommended above, at Recommendations 3 and 4, will assist in addressing these types of concerns.

48. There are also deeper concerns about the ways in which the harvesting of personal information potentially violates human rights – in addition to the role that such harvested information may play in potentially assisting foreign interference operations.

49. Key to addressing these concerns is ensuring that social medial platforms are transparent about the way that they collect and use personal information, and ensuring that there is consent by individual users. The right to privacy extends to the online space, including social media. Australians using social media have a right to understand what personal data they are being asked to hand over, and to expect that it will be protected.

50. In 2022, the Australian government proposed stronger penalties for repeated or serious privacy breaches[35] and the Attorney-General has recently received the review of the *Privacy Act 1988* (Cth) and announced that significant reforms will be introduced to modernise the Act that he has described as 'out of date and not fit-for-purpose in our digital age'.[36] The Commission looks forward to engaging in any future consultation processes around these proposed reforms.

51. Ensuring that the personal data which is collected about Australians by social media platforms is not excessive and is adequately safeguarded from potential exploitation by third parties (including foreign state actors),

is another critical aspect of ensuring that the right to privacy is protected. An important first step is knowing where the personal data that is collected is stored, who potentially has access to that data, and what protections are in place to prevent its misuse.

52. Recent research into data collection and access at TikTok highlights the urgency of understanding these risks and taking effective action to protect both individual Australian users and Australia's national security interests. For example, technical analysis of the source code of TikTok mobile applications conducted by Internet 2.0 in July 2022 revealed excessive data harvesting and that TikTok IOS 25.1.1 had a direct server connection to mainland China.[37]

53. TikTok is owned by the Chinese company ByteDance, with the close links between ByteDance and the Chinese Communist Party being the subject of previous reporting.[38] TikTok has consistently assured Australian policy makers that Australian user data is stored in Singapore, with strict protocols in place to protect access to that data.[39] However, in July 2022 it was confirmed that while TikTok claim never themselves to have provided Australian user data to the Chinese government, internal access to Australian user data is provided to employees 'wherever they're based, based on need'.[40] While TikTok have claimed that this access is strictly limited and subject to a series of robust controls, it does leave open the real possibility of Australian user data being accessible in mainland China. Given the operation of Chinese national security laws, such as the National Intelligence Law of 2017, this raises the prospect of Chinese-based employees being compelled to cooperate with Chinese intelligence agencies and sharing Australian user data without TikTok necessarily being aware that this has occurred.

54. Similar concerns have been raised in other countries. For example, Forbes recently reported 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.[41] This followed an earlier investigation by BuzzFeed News that concluded China-based TikTok employees had access to US user data, and repeatedly accessed that data.[42]

55. Concerns of this nature have resulted in bans on the use of TikTok on government-issued devices being introduced by the federal government and nearly half of the states in the USA,[43] as well the Netherlands issuing general advice to suspend the use of TikTok for the government until data protection policies have been adjusted.[44] It has been reported that a number of Australian government departments have banned the use of

TikTok on work-issued devices,[45] while Federal Ministers and Senators have also been warned about installing apps such as TikTok.[46]

56. In light of these security concerns, it would be appropriate for the Australian government to audit the use of social media platforms on government-issued devices within the Australian Public Service, and to issue clearer guidance regarding device security (including guidance regarding any social media platforms that should not be downloaded or used on government-issued devices).

57. While recent concerns have been highlighted with respect to TikTok, ensuring user data privacy and user data protections is a general concern with regards to the use of social media. Whilst Tiktok has been subject to particular scrutiny in recent times, it is important to remain vigilant with respect to the privacy risks posed by all online platforms. Policy responses to this issue should not specifically target individual companies, but instead apply to all social media companies to ensure that the same protections are extended to all Australian social media users, regardless of the specific platform they choose to use.

**Recommendation 5: The Australian Government should audit the use of social medial platforms on government-issued devices within the Australian Public Service, and issue general guidance regarding device security**.

58. While there are a range of existing laws, guidelines and strategies that apply to various aspects of privacy, the use of data, and cyber-security in Australia, there is a significant regulatory gap in respect of risks outlined above and the specific context of social media and internet companies. The Commission supports the recommendation previously made by the Australian Strategic Policy Institute that the Australian Government should introduce transparent user-data privacy and user-data protection frameworks that apply to all social media and internet companies. Any company that refuses to comply with such frameworks should not be able to operate in Australia.[47]

**Recommendation 6: The Australian Government should introduce transparent user-data privacy and user-data protection frameworks that apply to all social media and internet companies.**

59. The Commission also supports individuals being given greater control over how their personal data is used, and would support social media platforms being legally required to do this. In particular, a user's data-sharing settings should always be switched off by default.

**Recommendation 7: Social media platforms should be legally required to provide users with greater control over their personal data. A user's data-sharing settings should always be switched off by default.**

## 3.3 Censorship

60. 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.

61. The right to freedom of expression is often challenged in digital commons as users to seek to express their views on a wide range of topics – from politics to religion to art online. However, there is often a competing tension on where to draw the line between freedom of expression and content moderation. This is a line where reasonable minds may differ – however moderation should not unduly impact free speech, nor should hateful content be allowed to prosper under the guise of freedom of expression. Equally when considering any responses to the challenges posed to democracy by foreign interference operations, policy makers must ensure that people's right to participate in public affairs is not inappropriately impeded.

62. This extends to undue scrutiny of particular communities, most notably Chinese communities in Australia, which could impede their right to freedom from discrimination and freedom of expression. The unfair targeting of Chinese communities as a consequence of concerns about foreign interference in Australia must be assiduously avoided - as it risks exacerbating anti-Asian sentiment. This sentiment has been heightened since the COVID-19 pandemic and undermines the belonging of Chinese Australians (and those who are racialised as Chinese), their participation in public life and their ability to thrive in this country.

63. Attempts at extraterritorial censorship can have a direct impact on the human rights of Australians or those living in Australia, as well as

undermining Australia's democracy. Some examples that have come to the attention of the public in recent times include:

- Australian pro-democracy protestors reporting family in Iran being arrested and questioned about their relatives' actions in Australia, (including their social media communications).[48]
- Allegations of intimidation, harassment and surveillance of Chinese and Hong Kong students on Australian university campuses, including through the use of social media.[49]
- Allegations that TikTok engages in censorship on a range of political and social topics, with leaked content moderation documents suggesting TikTok has instructed its moderators to 'censor videos that mention Tiananmen Square, Tibetan independence or the banned religious group Falun Gong'.[50]

64. 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'.[51]

**Recommendation 8: The Australian Government should mandate that all social media platforms publicly disclose the content that they censor and make it an offence to censor content where that has not been publicly disclosed to users.**

65. With respect to the first two examples, we would note particularly Recommendation 2 from the First Interim Report which recommended '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'. The Commission supports this recommendation for the reasons outlined in the First Interim Report as an important measure for protecting both individuals and diaspora groups from foreign interference and extraterritorial censorship.

**Recommendation 9: The Australian Government should take a proactive approach to protecting groups that are common targets of foreign interference but are not classified as government institutions.**

# 4 Recommendations

**Recommendation 1**

The Australian Government should establish a permanent whole-of-government taskforce dedicated to preventing and combating foreign interference by way of cyber-manipulation in Australia.

**Recommendation 2**

The Australian government should establish clear and mandatory requirements, and pathways, for social media organisations to report suspected foreign interference. Such reports should be made to the proposed entity noted above in Recommendation One, whose activities in this area must incorporate robust safeguards to protect freedom of expression.

**Recommendation 3**

There must be greater investment in incorporating digital literacy into the Australian education curriculum, including information about online safety, data privacy, identifying misinformation and disinformation and the role algorithms play in a users' online experience.

**Recommendation 4**

The Australian Government should introduce a public education campaign on digital literacy, and develop online digital literacy resources that are available to the general public.

**Recommendation 5**

The Australian Government should audit the use of social medial platforms on government-issued devices within the Australian Public Service, and issue general guidance regarding device security.

**Recommendation 6**

The Australian government should introduce transparent user-data privacy and user-data protection frameworks that apply to all social media and internet companies.

**Recommendation 7**

Social media platforms should be legally required to provide users with greater control over their personal data. A users' data sharing setting should always be switched off by default.

**Recommendation 8**

The Australian Government should mandate that all social media platforms publicly disclose the content that they censor and make it an offence to censor content where that has not been publicly disclosed to users.

**Recommendation 9**

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

## Endnotes

[1] Electoral Integrity Assurance Taskforce, *Disinformation and Misinformation Factsheet* <eiat-disinformation-factsheet.pdf (aec.gov.au)>.
[2] Select Committee on Foreign Interference through Social Media Interim, *First Interim Report* (First Interim Report, December 2021), 12 [2.7].
[3] Electoral Integrity Assurance Taskforce, *Foreign Interference Factsheet* <eiat-foreign-interference-factsheet.pdf (aec.gov.au)>.
[4] Ibid.
[5] Genroe, *Social Media Statistics for Australia* (July 2022) <Social Media Statistics for Australia (Updated July 2022) - Genroe>.
[6] Dr Jake Wallis, International Cyber Policy Centre, Australian Strategic Policy Institute ('ASPI'), *Committee Hansard*, 22 June 2020, 10.
[7] Sarah O'Connor, Fergus Hanson, Emilia Currey and Tracy Beattie, *Cyber-enabled Foreign Interference in Elections and Referendums* (ASPI, 2020) 6.
[8] Select Committee on Foreign Interference through Social Media Interim, *First Interim Report* (First Interim Report, December 2021) 23 [3.3].
[9] Ibid 34 [4.14].
[10] Australian Security Intelligence Organisation, *2020-21 Annual Report* (Australian Security Intelligence Organisation, 19 October 2021) 4.
[11] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1976 (entered into force 23 March 1976) 999 UNTS 171 and 1057 UNTS 407 art 19.
[12] Ibid art 17.
[13] Ibid art 25.
[14] V-Dem Institute, *Democracy Report 2022: Autocratization Changing Nature?* (University of Gothenburg, March 2022) 35.
[15] News and Media Research Centre, Submission No 8 to Senate, *Select Committee on Foreign Interference through Social Media* (2021) 2-3.

[16] Sora Park et al., *Digital News Report: Australia 2022* (News and Media Research Centre, June 2022) 71.
[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Select Committee on Foreign Interference through Social Media Interim, *First Interim Report* (First Interim Report, December 2021).
[21] Department of Home Affairs, Submission No 16 to *Senate Select Committee on Foreign Interference through Social Media* (2021), 7.
[22] V-Dem Institute, *Democracy Report 2022: Autocratization Changing Nature?* (University of Gothenburg, March 2022) 35.
[23] Transparency reports were published by Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitter, and can be found at <TRANSPARENCY | DIGI>.
[24] UN Human Rights Committee, *General Comment No 34 (Article 19: Freedom of opinion and expression)*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011), [21].
[25] See *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd session, 183 plen mtg, UN Doc A/810 (10 December 1948) art 12; *International Covenant on Civil and Political Rights*, opened for signature 16 December 1976 (entered into force 23 March 1976) 999 UNTS 171 and 1057 UNTS 407 art 17; *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 16.[26] Select Committee on Foreign Interference through Social Media Interim, *First Interim Report* (First Interim Report, December 2021) 24 [3.7].
[27] Ibid 32 [4.6].
[28] Ibid 45 [4.49].
[29] Responsible Technology Australia, Submission No 17 to Senate, *Select Committee on Foreign Interference through Social Media* (2021) 2.
[30] Select Committee on Foreign Interference through Social Media Interim, *First Interim Report* (First Interim Report, December 2021) 26 [3.16].
[31] The Department of Home Affairs, Submission No 16 to Senate, *Select Committee on Foreign Interference through Social Media* (2021) 4; see also The Allens Hub for Technology, Law and Innovation, Submission No 19 to Senate, *Select Committee on Foreign Interference through Social Media* (2021) 2.
[32] Select Committee on Foreign Interference through Social Media Interim, *First Interim Report* (First Interim Report, December 2021) 24-25 [3.10].
[33] The Allens Hub for Technology, Law and Innovation, Submission No 19 to Senate, *Select Committee on Foreign Interference through Social Media* (2021) 4.
[34] Australian Electoral Commission, Submission No 120 to the Joint Select Committee on Electoral Matters, *Inquiry into and Report on All Aspects of the Conduct of the 2019 Federal Election and Matters Related Thereto* (2018) 32.
[35] *Privacy Legislation Amendment (Enforcement and Other Measures) bill 2022* (Cth).
[36] Paul Karp, 'Australia to consider European-style right to be forgotten privacy laws', *The Guardian,* 19 January 2023. <Australia to consider European-style right to be forgotten privacy laws | Australian politics | The Guardian>.
[37] Thomas Perkins, *Internet 2.0 TikTok Analysis* <It's their word against their source code - TikTok report - Internet 2.0 (internet2-0.com)>.

[38] See, for example, Fergus Ryan, Audrey Fritz and Daria Impiombato, *TikTok and WeChat: Curating and controlling global information flows,* (Australian Strategic Policy Institute, International Cyber Policy Centre, Policy Brief Report No. 37/2020), 49 – 50.
[39] See, for example, Evidence to Senate Select Committee on Foreign Interference Through Social Media, Parliament of Australia, Canberra, 25 September 2020 (Roland Cloutier, Lee Hunter and Brent Thomas). 10 – 22.
[40] Letter from Mr Brent Thomas (Director of Public Policy, Australia and New Zealand, TikTok) to Senator James Paterson (Shadow Minister for Cyber Security), 12 July 2022.
[41] Emily Baker-White, 'TikTok Spied on Forbes Journalists', *Forbes,* 22 December 2022. <EXCLUSIVE: TikTok Spied On Forbes Journalists>.
[42] Emily Baker-White, 'The TikTok Tapes', *BuzzFeed News,* 18 June 2022. <US TikTok User Data Has Been Repeatedly Accessed From China, Leaked Audio Shows (buzzfeednews.com)>.
[43] Scott Bauer, 'Wisconsin, North Carolina governors ban popular TikTok app', *AP News,* 13 January 2023. <Wisconsin, North Carolina governors ban popular TikTok app | AP News>.
[44] Pieter Haeck, 'Don't use TikTok, Dutch officials are told', *Politico,* 25 January 2023. <Don't use TikTok, Dutch officials are told – POLITICO>.
[45] Nick Bonyhady, 'Two more federal government departments ban TikTok', *WA Today*, 02 February 2023. < https://www.watoday.com.au/technology/two-more-federal-government-departments-ban-tiktok-20230201-p5ch5o.html>.
[46] Max Mason, 'Federal MPs, senators warned about installing apps 'such as TikTok'', *Australian Financial Review*, 10 February 2023. <https://www.afr.com/technology/federal-mps-senators-warned-about-installing-apps-such-as-tiktok-20230210-p5cjnr>.
[47] Fergus Ryan, Audrey Fritz and Daria Impiombato, *TikTok and WeChat: Curating and controlling global information flows,* (Australian Strategic Policy Institute, International Cyber Policy Centre, Policy Brief Report No. 37/2020), 48.
[48] Paul Sakkal, 'Silencing dissent by threatening family': Iran cracks down on family of Australian protester, *The Sydney Morning Herald,* 16 January 2023. <Iran cracks down on family of Australian protesters (smh.com.au)>
[49] Human Rights Watch, 'They Don't Understand the Fear We Have: How China's Long Reach of Repression Undermines Academic Freedom at Australia's Universities' (2021) <australia0621_reportcover_8.5x11 (hrw.org)>,
[50] Fergus Ryan, Audrey Fritz and Daria Impiombato, 'TikTok and WeChat: Curating and controlling global information flows' (ASPI International Cyber Policy Centre, Policy Brief Report No. 37/2020), 9 – 10. <TikTok and WeChat: Curating and controlling global information flows>.
[51] Ibid 48.