



Australian Government
Department of Home Affairs

Department of Home Affairs Submission to the Select Committee on Foreign Interference through Social Media

Select Committee on Foreign Interference through Social Media

17 February 2023

Table of Contents

Overview	3
Social media companies	3
2022 Australian Federal Election	4
Department of Home Affairs initiatives	4
Complementary initiatives	5
Conclusion	6

Overview

1. The Department of Home Affairs (the Department) welcomes the opportunity to provide an addendum to the 2021 Submission to the Select Committee on Foreign Interference through Social Media.
2. 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.
3. In 2022, the Director General of the Australian Security Intelligence Organisation (ASIO) stated that over the past two years, thousands of Australians with access to sensitive information have been targeted by foreign spies using social media profiles.

Social media companies

4. Social media companies have a critical role in identifying and responding to information operations. Between 2017 and 2022, Meta disabled and publicly reported on over 200 covert influence operations that violated its policies.¹ These operations originated from over 60 countries and targeted both foreign nations and their own domestic public debate. In another report from September 2022, Meta outlined its actions to take down two unconnected information operations sourced from within Russia and China that violated Meta's policies.²
5. Social media companies can have a significant role in moderating how foreign actors seek to exploit their platforms to conduct information operations. Research by Global Witness and the Cybersecurity for Democracy team at New York University found weaknesses in TikTok's and Meta's ability to effectively moderate 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.³ Similar studies conducted globally, indicate social media platform content moderation success can vary from one country to another.
6. Employees of social media platforms can misuse their access to personal data. In December 2022, a former Twitter employee in the United States was sentenced to 42 months in federal prison for his role in accessing sensitive information that could be used to identify and locate Twitter users of interest to the Saudi Royal Family.⁴
7. The Australian information environment is not immune from threats of foreign interference through social media. Publicly available reporting by the Australian Strategic Policy Institute (ASPI) found that women of Asian descent living in democracies around the world, including Australia, the United

¹ "Recapping Our 2022 Coordinated Inauthentic Behavior Enforcements", Meta, December 2022, online at: [Recapping Our 2022 Coordinated Inauthentic Behavior Enforcements | Meta \(fb.com\)](#)

² "Taking down coordinated inauthentic behaviour from Russia and China", Meta, September 2022, online at: [CIB-Report -China-Russia-Sept-2022.pdf \(fb.com\)](#)

³ "Summary of findings: TikTok and Facebook fail to detect election disinformation in the U.S., while YouTube succeeds", Cybersecurity for Democracy, 21 October 2022, online at: [Cybersecurity for Democracy](#)

⁴ "Former Twitter Employee Sentenced to 42 Months in Federal Prison for Acting as a Foreign Agent", The United States Department of Justice, 15 December 2022, online at: [Former Twitter Employee Sentenced to 42 Months in Federal Prison for Acting as a Foreign Agent | OPA | Department of Justice](#)

Kingdom, and the United States, have been targeted by ongoing coordinated information operations.⁵ ASPI has separately reported that Australian mining company Lynas Rare Earths was targeted by information operation that used environmental, political and health concerns to undermine efforts to diversify global rare-earth supply chains.⁶

2022 Australian Federal Election

8. In preparation for the 2022 Federal Election, relevant Electoral Integrity Assurance Taskforce (EIAT) members engaged with Australian representatives from Meta, Google, Snap, Tencent, TikTok, Twitter, Microsoft and Reddit. The AEC established a framework with Meta, Twitter, Google, Microsoft and TikTok for operational arrangements allowing the AEC and the Electoral Integrity Assurance Taskforce to refer harmful electoral content to online platforms for consideration and removal, where content was in breach of relevant legislation or the platform's own policies.
9. The AEC has acknowledged the success of these relationships, the support received from online platforms to combat misinformation, and their assistance in maintaining the integrity of the 2022 federal election.
10. Additionally, the Australian Electoral Commission implemented a number of measures to combat mis- and disinformation, including a nationwide education and advertising campaign, establishing a disinformation register, referring mis- and disinformation to major online platforms for review against their terms of service or Australian electoral law, and responding directly to mis- and disinformation online, primarily via Twitter.
11. As stated by the Australian Electoral Commissioner, Mr Tom Rogers, on 26 July 2022, EIAT *"agencies did not identify any foreign interference, or any other interference, that compromised the delivery of the 2022 Federal Election and would undermine the confidence of the Australian people in the results of the election"*.

Department of Home Affairs initiatives

12. The Department continues to engage 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. The Department's engagement informs Australia's domestic policies and legislative frameworks to protect Australian interests from hostile state actor activities, and complements the work of other relevant government agencies.
13. The Department uses an integrated model to counter mis- and disinformation online and offline, in English and other community languages. It includes:
 - a. the Australian Values social media channels which provide information about Australia's values as a liberal democracy, and helps communities build awareness and resilience to disinformation;
 - b. partnerships with other government agencies, non-government organisations, and community members to provide regular and ongoing information and messaging about Australia's values and Australia's inclusive national identity, and to counter mis- and disinformation;

⁵ 'Smart Asian women are the new targets of CCP global online repression', Australian Strategic Policy Institute, 3 June 2022, online at: [Smart Asian women are the new targets of CCP global online repression | The Strategist \(aspistrategist.org.au\)](https://www.aspi.org.au/the-strategist/smart-asian-women-are-the-new-targets-of-ccp-global-online-repression)

⁶ "The CCP's information campaign targeting rare earths and Australian company Lynas", Australian Strategic Policy Institute, 29 June 2022, online at: [The CCP's information campaign targeting rare earths and Australian company Lynas | The Strategist \(aspistrategist.org.au\)](https://www.aspi.org.au/the-strategist/the-ccps-information-campaign-targeting-rare-earths-and-australian-company-lynas)

- c. community liaison teams that engage with culturally and linguistically diverse communities to counter mis- and disinformation with the facts;
 - d. monitoring trends in the information environment that could impact Australia's social cohesion and democratic principles; and
 - e. referrals of COVID-19 mis- and disinformation to social media platforms for review against their terms of service.
14. In September 2022, the Minister for Home Affairs requested the Department undertake a review of the security risks social media platforms present and the settings which govern them. The *review into Foreign Interference through Social Media Applications* (the Review) will consider all options to address data security risks, as well as mis- and disinformation concerns as they relate to social media platforms. The Review will consider all social media platforms available to Australians and will be delivered to the Minister for Home Affairs in the first quarter of 2023.
 15. The Australian Government is developing Australia's first *Data Security Action Plan* and it is proposed as a key initiative under the *Cyber Security Strategy 2023-2030*. The Action Plan will seek to strengthen data security policy settings across Government and the broader economy, and will leverage existing and ongoing efforts to uplift data security across industry, states and territories. The storage settings of domestic and international data and whether they adequately promote privacy, security and transparency, are being considered in the development.
 16. The Department's Strengthening Democracy Taskforce aims to identify initiatives to bolster Australia's democratic resilience and enhance trust among citizens, and between citizens and governments. The Taskforce will engage across Australian society and work in partnership with Australian civil society organisations. The Taskforce will draw on empirical data, research, and diverse perspectives to deliver a practical, innovative agenda for sustaining and strengthening our democratic resilience, in the near term and for the long term. The newly established National Resilience Taskforce will also work closely with the Strengthening Democracy Taskforce, noting Australia's democratic resilience underpins our national resilience.

Complementary initiatives

17. In March 2022, RMIT University's RMIT FactLab announced it was joining Meta's third-party fact checking program. They will "*review and rate the accuracy of social media posts that relate to Australia*", expanding their existing efforts to reduce the spread of misinformation online. This is in addition to the ongoing partnership between RMIT and the ABC to produce the 'RMIT ABC Fact Check', which tests the claims of public figures and institutions.
18. SBS language services give vital, reliable information about current events to CALD communities within Australia, who are particularly vulnerable to the impacts of misinformation, as well as offering an Australian perspective to audiences across the globe. By presenting truthful information in understandable formats for non-English audiences, the SBS programs help to improve social cohesion and counter foreign interference. SBS broadcasts in 68 different languages and reaches large segments of Australia's multicultural and multilingual communities.
19. The Australian Cyber Security Centre monitors cyber security threats and provides publicly available advice and information to individuals and families, small and medium-sized businesses, organisations and critical infrastructure, and the Government, to appropriately protect themselves. The Centre shares security tips for personal and business use to ensure users secure their social media accounts and are aware of the risks of social media and messaging apps.

20. In the October 2022-23 Budget, the Australian Government committed \$6 million 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.
21. On 20 January 2023, the Hon Michelle Rowland MP, Minister for Communications, announced that the Government will provide the Australian Communications and Media Authority (ACMA) with new powers to combat mis- and disinformation on digital platforms. This legislative reform will include providing the ACMA with information gathering, record keeping and reserve code and standard making powers. The powers will allow the ACMA to increase platform transparency on measures to combat mis- and disinformation, including mandating platforms to keep and provide it with data on Australia-specific measures.

Conclusion

22. Foreign actors continue to develop methods to conduct information operations and spread mis- and disinformation through social media in order to advance their own interests at the expense of Australia.
23. The social media landscape in Australia continues to evolve. Contemporary Australia's widespread use and reliance on social media, matched with the speed information can be created, captured and shared, highlight the significance of the matter. Appropriate regulation, engagement with social media platforms by government, and public media literacy, will provide a foundation to resist online threats by foreign actors.