

Submission on Foreign Interference through Social Media

31 October 2021

Senate Select Committee on Foreign Interference through Social Media

By email: foreigninterference.sen@aph.gov.au

Contact: **Simon Bruck**
President, NSW Young Lawyers

Olivia Irvine
Chair, NSW Young Lawyers Communications, Entertainment and Technology Law Committee

Joshua Clarke
Chair, NSW Young Lawyers International Law Committee

Contributors: Anjali Nadaradjane, Madeleine Gandhi, Anagha Bidkar and Caitlyn Allen

Co-ordinators: Taylah Spirovski and Caitlyn Allen

The NSW Young Lawyers Communications, Entertainment and Technology Law Committee and the International Law Committee (the Committees) make the following submission on Foreign Interference through Social Media.

NSW Young Lawyers

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 15 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers (solicitors and barristers) under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

NSW Young Lawyers Communications Entertainment and Technology Law Committee

The NSW Young Lawyers Communications, Entertainment and Technology (**CET**) Committee aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to information and communication technology (including technology affecting legal practice), intellectual property, advertising and consumer protection, confidential information and privacy, entertainment, and the media. As innovation inevitably challenges custom, the CET Committee promotes forward thinking, particularly with respect to the shape of the law and the legal profession.

NSW Young Lawyers International Law Committee

The International Law Committee is committed to providing a platform to young lawyers and law students with a key interest in international law (both public and private) to discuss among peers and learn from experts in the field through selected seminars, as well as providing networking opportunities. The Committee currently has over 1,200 members and has established working relationships with the Australian Institute of International Affairs, the Australian Dispute Centre, the Australian Centre for International Commercial Arbitration and the Rule of Law Institute of Australia. As one of its primary goals, the Committee endeavours to broaden the knowledge of international law within the legal profession and the Australian legal system. In doing so, the Committee seeks to promote informed discussion amongst its members and the wider legal community on international law in Australia.

Introduction

The Committees welcome the opportunity to comment on Foreign Interference through Social Media on behalf of NSW Young Lawyers. The Terms of Reference consider the risk posed to Australia's democracy by foreign interference through social media, with particular reference to:

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

The Committees have responded to parts (a) and (c) of the Terms of Reference in this submission and have otherwise not made submissions on the remaining Terms of Reference here. The Committees further rely on the NSW Young Lawyers submission made on 13 March 2020.¹

Summary of Recommendations

1. The Committees submit that the Australian Government should create easily digestible material that educates the public on detecting and differentiating fake social media accounts, particularly social bots.
2. The Committees submit that the Australian Government should require social media outlets operating in Australia to implement a policy that mandates the imposition of adequate checks and balances, and transparency to monitor the role of algorithms in the spread of misinformation and manipulated content.
3. The Committees submit that the Australian Government should require particular social media outlets, such as WeChat and Twitter, publish a digital registry of information for paid content.

¹ NSW Young Lawyers, International Law Committee Submission to the Select Committee on *Foreign Interference through Social Media* (13 March 2020) 5 <https://www.lawsociety.com.au/sites/default/files/2021-04/20200313_Submission_to_the_Select_Committee_on_Foreign_Interference_th.pdf>.

4. The Committees recommend the Australian Government expands upon the Australian Electoral Commission's (AEC's) powers, to provide it with the authority to compel social media companies to provide information relevant to its investigations within specified timeframes. If those requests are not met with compliance within the specified timeframe, then punitive measures should be available, such as penalties and sanctions until compliance is met.
5. The Committees recommend amending the *Broadcasting Services Act 1992* (Cth) to modernise campaign methods by expanding the relevant provisions to include social media and online advertising.
6. The Committees recommend the Electoral Integrity Assurance Task Force take a more proactive approach in investigating and exposing cases of foreign interference.
7. The Committees recommend the Electoral Integrity Assurance Task Force implement an online searchable platform where previous cases of misinformation and interference are listed to increase public awareness.
8. The Committees recommend the Australian Government strengthen measures to educate the public on misinformation and provide the necessary skills to ascertain the validity of information presented. Programs such as the AEC's 'Stop and Consider' campaign are useful tools, however, other programs should be implemented and encouraged, including through integration of similar content in the education system to better educate the next generation on the tools they can utilise to help verify accurate information presented in cyber platforms.

Part A - use of social media for purposes that undermine Australia's democracy and values, including the spread of misinformation

1. The Committees submit that, without safeguards, social media is a ready tool to cultivate social division and influence political processes through misinformation and disinformation. Social media cyber-operations present an immense challenge to the international community, especially given that

customary international laws and formal agreements in respect of cyber-operations are still developing.²

2. The Committees define misinformation in this submission as false or inaccurate information that is not created with the intention of causing harm, and disinformation as false or misleading information that is deliberately disseminated by methodologies including spam campaigns and/or bots to mislead or deceive its recipients.³

Social Bots

3. Social bots are automated or semi-automated social media accounts which are primarily controlled by algorithms, and which are programmed to behave like human social media users (for example, by automatically generating and spreading content).⁴ The coordinated use of social bots can influence public opinion by giving the false impression that masses of *human* users support a particular idea or political candidate.
4. The Committees submit that the Australian Government should create digestible material that educates the public on how to detect and differentiate fake social media accounts from genuine accounts, particularly how to identify the use of social bots.⁵
5. Social bots are prevalent on social networks, with bots representing up to 25 percent of all Twitter accounts and a large portion of Facebook accounts.⁶ Concerningly, this figure is likely to increase because bots are becoming easier to create due to rapid advancements in technology. At present, users without in-depth programming skills are still able to create bots through application programming interfaces and online services such as Somiibo.⁷
6. The Committees wish to emphasise research conducted by the Australian Strategic Policy Institute, which identifies Russia as the most prolific state actor engaging in online interference, followed by

² Ashley Nicolas, 'Taming the Trolls: The Need for an International Legal Framework to Regulate State Use of Disinformation on Social Media' (2018) 107 *Georgetown Law Journal Online* 36, 38.

³ Australian Communications and Media Authority, *Misinformation and news quality on digital platforms in Australia: A position paper to guide code development* (Report, June 2020) 9-10.

⁴ Maja Brkan, 'Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting' (2019) 2(2) *Delphi Interdisciplinary Review of Emerging Technologies* 66, 66-67.

⁵ Sanja Kelly et al, 'Manipulating Social Media to Undermine Democracy', *Freedom House* (Webpage) <<https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy>>.

⁶ *Ibid.*

⁷ *Ibid.*

China, Iran and North Korea.⁸ These governments rely on a 'complex production and dissemination apparatus... to enable large-scale and complex information operations' targeting democratic institutions, public opinion and civilian infrastructure.⁹ This 'apparatus' involves the use of fake social media accounts (including social bots and 'troll farms') to amplify false news stories from state-controlled and state-censored media outlets.¹⁰ For example, it is estimated that 2.12 million tweets about the 2016 US election originated from malicious Russian-linked accounts.¹¹ The Committees submit that the Australian Government should consider these examples as case studies of a global trend.

7. The Committees submit that the Australian Government should take proactive steps to improve public awareness, and media literacy regarding the presence, effect, and detection of social bots and troll farms. The Committees note that while the detection of bots has increasingly become a specialised area of research,¹² (particularly with new classes of bots multiplying at a speed difficult to monitor) it is nevertheless important that the public are provided with tools to improve their social media literacy to ensure that they can critically appraise the information being disseminated.

Social media algorithms amplify malicious content

8. The Committees submit that the Australian Government should require social media outlets operating in Australia to implement a policy which mandates the imposition of adequate checks and balances, and transparency to monitor the role of its algorithm in the spread of misinformation and manipulated content.¹³

⁸ Danielle Cave and Jake Wallis, 'Defending democracies from disinformation and cyber-enabled foreign interference', *Australian Strategic Policy Institute* (online, 22 April 2021) <<https://www.aspistrategist.org.au/defending-democracies-from-disinformation-and-cyber-enabled-foreign-interference/>>.

⁹ Todd Helmus et al, 'Russian Social Media Influence, Understanding Russian Propaganda in Eastern Europe' RAND Corporation (2018) 11.

¹⁰ Jonathan Schnader, 'Accounting for Foreign Disinformation: National Security Regulatory Proposals for Social Media Accounts and False Speech' (2021) 36(1) *Journal of Law & Politics* 1, 10.

¹¹ Open Hearing on Foreign Influence Operations' Use of Social Media Platforms (Company Witnesses): Hearing Before the Senate Select Committee on Intelligence, 115th Cong. 22 (2018) (testimony of Jack Dorsey, Chief Executive Officer, Twitter, Inc.).

¹² Franziska Martini et al, 'Bot, or not? Comparing three methods for detecting social bots in give political discourses' (2021) 8(2) *Big Data & Society* 1, 3.

¹³ Yaël Eisenstat, 'How to Hold Social Media Accountable for Undermining Democracy', *Harvard business Review* (Web page, 11 January 2021) <<https://hbr.org/2021/01/how-to-hold-social-media-accountable-for-undermining-democracy>>.

Viral by design

9. The Committees submit that an integral part of proactive social media surveillance is understanding and exploring malicious actors who exploit social media algorithms to maximise the reach of manipulated content, such as 'deepfakes'. Deepfake technologies enable the manipulation of audio-visual material to depict events that never happened, including creating realistic audio/video recordings of people, and are increasingly sophisticated in terms of believability due to advancements in artificial intelligence.¹⁴ Content produced by deepfake technology is often designed to be shocking because social media algorithms generally filter and prioritise content shown to users with a focus on maximising user-engagement. As a result, 'deep-fakes' have a strong tendency to go 'viral' and rapidly reach wide audiences.

Inadequate checks and balances

10. The Committees wish to highlight a range of risks which the Australian Government faces if adequate checks and balances of social media are not put in place.
11. Social networks are designed to maximise user-engagement rather than detect falsehoods and inaccuracies. Moreover, unlike traditional print media, the publication of online content is not subject to verification processes and editorial standards. As a result, false news stories are freely disseminated in the public domain; for example, false reports that Pope Francis had endorsed Donald Trump's 2016 presidential candidacy attracted 960,000 Facebook engagements over one month.¹⁵ Mark Zuckerberg himself has acknowledged that Facebook 'didn't do enough'¹⁶ to prevent the misuse of the platform to spread fake news, hate speech, and facilitate foreign interference in elections.¹⁷
12. Over a ten-year period, false news content on Twitter has 'diffused significantly further, faster, deeper and more broadly than the truth'.¹⁸

¹⁴ Maja Brkan, 'Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting' (2019) 2(2) *Delphi - Interdisciplinary Review of Emerging Technologies* 66.

¹⁵ Hannah Ritchie, 'Read All About It: The Biggest Fake News Stories of 2016' *CNBC* (online, 30 December 2016) <<https://www.cnn.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html>>.

¹⁶ Facebook, Social Media Privacy, and the Use and Abuse of Data: Joint Hearing Before the S Comm. on the Judiciary, S. Comm. on Commerce, Sci., & Transp., 115th Cong. 8 (2018) (testimony of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook).

¹⁷ *Ibid.*

¹⁸ Soroush Vosoughi et al, 'The Spread of True and False News Online' (2018) 359 *Science* 1146, 1146-1151.

13. In Australia, the scale and impact of 'fake news', and the ease with which malignant actors can manipulate open information environments, is compounded by relatively low rates of media literacy in society.¹⁹

Part C - international policy responses to cyber-enabled foreign interference and misinformation

14. It is a delicate balancing act to ensure that human rights, the right to privacy and freedom of speech are continually being upheld and not undermined by totalitarian measures that extend past the necessary protective intentions of the legislation. The right to hold opinions without interference is protected by the *International Covenant on Civil and Political Rights (ICCPR)*.²⁰ Freedom of opinion and freedom of expression are the two pillars of every free and democratic society,²¹ enforcement of legislation must ensure not to encroach on these foundations. In a recent case, *Zhang v Commissioner of Police*,²² the validity of the current legislative framework in *Criminal Code Act 1995 (Cth)* under section 92.3(1) and (2)²³ was challenged as a breach of implied political freedoms. However, the judgement deemed this issue "unnecessary to answer", resulting in uncertainty as to the existence and functionality of the right to political freedom and freedom of expression.²⁴ Unfortunately, the encroachment of legislation on implied rights remains unanswered. Therefore the balancing act is ensuring that political rights and freedoms are protected while ensuring that Australia's democracy is free from foreign interference especially through cyber-enabled misinformation.
15. One example of foreign interference impacting the democratic right of political communication in Australia was during the same-sex plebiscite, when a Panama registered, US hosted website published and advertised homophobic material to support the 'no' campaign in contravention of Australian electoral laws.²⁵ The AEC stated that it did not have sufficient resources to identify parties

¹⁹ See Tanya Notley et al, *Adult Media Literacy in Australia: Attitudes, Experiences and Needs* (Report, 14 April 2021); Jocelyn Nettlefold and Kathleen Williams, *Insight Five: A Snapshot of Media Literacy in Australian Schools* (Report, 3 September 2018).

²⁰ *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) art 19(1).

²¹ Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of opinion and expression to the International Covenant on Civil and Political Rights*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011).

²² *Zhang v Commissioner of Police* [2021] HCA 16, 33.

²³ *Ibid.*

²⁴ Belinda Baker, 'A court should be wary', *Aus Pub Law* (online, 16 June 2021) <<https://auspublaw.org/2021/06/a-court-should-be-wary-zhang-v-commissioner-of-police-2021-hca-16/>>

²⁵ Christopher Knaus and Nick Evershed, 'Electoral Watchdog Powerless to Crack Down on Offshore Political Ads Targeting Australians', *The Guardian* (Online, 24 July 2018) <<https://www.theguardian.com/australia-news/2018/jul/24/australian-watchdog-unable-to-enforce-political-advertising-law-over-offshore-sites>>

behind the campaign, or rectify the breach.²⁶ A further example of this interference is demonstrated in the lead up to the 2019 Federal Election, where research found that a Russian-linked troll farm was using Twitter to increase anti-Islamic sentiment and support for Julian Assange in Australia.²⁷

16. The impact of foreign interference in Australia is again magnified by an enforceability gap, where laws applying to communications on traditional media fail to appropriately engage with breaches on online media platforms. For example, Facebook failed to remove a political advertisement that did not display the required disclaimer during an election in a timely manner.²⁸ The AEC stated it had experienced difficulties with the responsiveness to their requests from social media companies more broadly.²⁹
17. In 2018, the Australian Government passed the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (**EFI Act**) which implemented foreign interference offences into the *Criminal Code Act 1995* (Cth).³⁰ The introduced offences aim to criminalise individuals who engage in misconduct with intent to influence or threaten political governmental processes.³¹ The amendment to the *Criminal Code*³² is a progressive step in modernising and adapting legal frameworks to protect Australian's democratic and political rights from foreign interference.³³
18. Many concerns have been identified since the introduction of the new offences.³⁴ The Law Council of Australia (**LCA**) expressed its concerns regarding the restrictive nature of the introduced offences, in particular the impact they may have on investigative journalism on behalf of foreign entities.³⁵ Another

²⁶ Ibid.

²⁷ Paul Karp, 'Russian Twitter trolls stoking anti-Islamic sentiment in Australia, experts warn' *The Guardian* (online, 20 November 2018) <<https://www.theguardian.com/australia-news/2018/nov/20/russian-twitter-trolls-stoking-anti-islamic-sentiment-in-australia-experts-warn>>.

²⁸ Joint Standing Committee on Electoral Matters, Parliament of Australia, *Australian Electoral Commission Annual Report 2017-18* (Status Report, March 2019) [3.19]-[3.23].

²⁹ Nick Evershed, 'Facebook took month to remove page that violated same-sex marriage safeguard laws', *The Guardian* (online, 2 November 2017) <<https://www.theguardian.com/technology/2017/nov/02/facebook-took-month-to-remove-page-that-violated-same-sex-marriage-safeguard-laws>>.

³⁰ *Criminal Code Act 1995*(Cth) sch 1 div 92.

³¹ Explanatory Memorandum, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018* [27].

³² *Criminal Code Act 1995* (Cth) sch 1 div 92.

³³ Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) <<https://www.lawcouncil.asn.au/docs/10bff746-c300-e811-93fb-005056be13b5/3390%20-%20National%20Security%20Legislation%20Amendment%20Espionage%20and%20Foreign%20Interference%20Bill%202017.pdf>>.

³⁴ NSW Young Lawyers, International Law Committee Submission to the Select Committee on *Foreign Interference through Social Media* (13 March 2020) 5 <https://www.lawsociety.com.au/sites/default/files/2021-04/20200313_Submission_to_the_Select_Committee_on_Foreign_Interference_th.pdf>.

³⁵ Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) 51 [157], <<https://www.lawcouncil.asn.au/docs/10bff746-c300-e811-93fb-005056be13b5/3390%20-%20National%20Security%20Legislation%20Amendment%20Espionage%20and%20Foreign%20Interference%20Bill%202017.pdf>>.

concern the LCA raised is the broad definition of select terms used within the new offences including but not limited to: 'inherently harmful information' and 'foreign intelligence agency'.³⁶ Other concerns raised include the fast-paced development of technology and the legislative deterrence framework's ability to respond to these rapid developments adequately to ensure all relevant conduct is captured.³⁷ For instance, under the *Broadcasting Services Act* in Australia, the media is subject to blackout times in relation to federal elections where they are unable to broadcast during those relevant periods.³⁸ Many broadcasting companies have since begun utilising their social media platforms to circumvent their licencing restrictions during relevant blackout periods, highlighting the limitations of technology specific drafting.³⁹

19. Foreign interference has posed challenges to democracy via the utilisation of misinformation and digital technology; however, these challenges are not unique to Australia. It is a constant global concern that many international governments have faced and have enacted relevant policies to attempt to mitigate the impacts of cyber-enabled misinformation. Australia would significantly improve its response to cyber-enabled interference and misinformation by observing and adapting its policies in accordance with the international community.
20. Australia's response requires alignment with current international obligations and respects fundamental legal human rights principles. The delicate balance between protection and curtailment of rights has not always been met, with some States' responses on this growing issue not taking fundamental human rights principles into consideration. Consequently, they have received criticism from the international community. Recently, Singapore introduced and passed the Foreign Interference (Countermeasures) Bill⁴⁰ with the purpose of "preventing, detecting and disrupting foreign

%20National%20Security%20Legislation%20Amendment%20Espionage%20and%20Foreign%20Interference%20Bill%202017.pdf> .

³⁶ Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) [221] <<https://www.lawcouncil.asn.au/docs/10bff746-c300-e811-93fb-005056be13b5/3390%20-%20National%20Security%20Legislation%20Amendment%20Espionage%20and%20Foreign%20Interference%20Bill%202017.pdf>> .

³⁷ NSW Young Lawyers, International Law Committee Submission to the Select Committee on *Foreign Interference through Social Media* (13 March 2020) 5 <https://www.lawsociety.com.au/sites/default/files/2021-04/20200313_Submission_to_the_Select_Committee_on_Foreign_Interference_th.pdf> .

³⁸ *Broadcasting Services Act 1992* (Cth), sch 2 s 3A.

³⁹ Danielle Long, 'Australia TV networks to stream political advertising online during election black out', *The Drum* (online, 13 May 2019) <<https://www.thedrum.com/news/2019/05/13/australia-tv-networks-stream-political-advertising-online-during-election-blackout>> .

⁴⁰ Human Rights Watch, *Withdraw Foreign Interference (Countermeasures) Bill* (Online at 13 October 2021) <Singapore: Withdraw Foreign Interference (Countermeasures) Bill | Human Rights Watch (hrw.org)> .

interference in domestic politics”.⁴¹ However, the broad construction of the legislation creates an overreach of executive power which impinges on the human rights of freedom of expression and privacy.⁴² Human Rights Watch requested withdrawal of this Bill on the grounds that it does not satisfy the principles of legality, necessity and proportionality recognised in international law.⁴³ These principles ensure that the individual human rights are maintained and the establishment of new laws are narrowly defined and directly related to the cause they were created to address.⁴⁴ It is crucial for Australia to consider these legal principles when developing new policies to address the issue of foreign interference and to ensure that the balance between human rights and the protection of Australia’s democracy is preserved.

21. Observing developments in Canada, the UK, the European Union (EU) and Ukraine provide opportunities to identify potential solutions which Australia may consider adapting. These are briefly discussed below.
22. The Canadian House of Commons produced a report addressing the threats and risks of disinformation, along with a range of recommendations to mitigate impacts of foreign interference.⁴⁵ Many of their recommendations involved increased education surrounding the impacts of foreign interference. Another recommendation was to increase transparency of political advertising by including identity authentication when publishing political advertisements online.⁴⁶ Australia has already implemented a transparency scheme known as the *Foreign Influence Transparency Scheme Public Register*.⁴⁷ However, as discussed above, Australia has relatively low media literacy rates, making the population vulnerable to misinformation in a digital context.⁴⁸
23. The UK has led numerous investigations and funded research schemes on the impacts of foreign interference through social media. Subsequently, the UK government has implemented legislative and

⁴¹ Ministry of Home Affairs Singapore, ‘*First Reading of Foreign Interference (Countermeasures) Bill*’ (online at 13 September 2021) <First Reading of Foreign Interference (Countermeasures) Bill (mha.gov.sg)>.

⁴² Human Rights Watch (n 40).

⁴³ Ibid.

⁴⁴ Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of opinion and expression to the International Covenant on Civil and Political Rights*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011).

⁴⁵ Canadian House of Commons Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat : Risks and Solutions in the Era of Disinformation and Data Monopoly* (Report, December 2018) <<https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf>>.

⁴⁶ Ibid.

⁴⁷ Australian Electoral Commission, ‘Electoral Integrity Assurance Taskforce’ (online, 9 June 2021) <<https://www.aec.gov.au/elections/electoral-advertising/electoral-integrity.htm>>.

⁴⁸ See Tanya Notley et al, *Adult Media Literacy in Australia: Attitudes, Experiences and Needs* (Report, 14 April 2021); Jocelyn Nettlefold and Kathleen Williams, *Insight Five: A Snapshot of Media Literacy in Australian Schools* (Report, 3 September 2018).

non-legislative responses to mitigate harms. Recommendations extracted from these investigations, *inter alia*, include the revision of the UK electoral law to cover 'modern' campaigning methods and to expand the powers of the electoral commission to compel social media companies to provide relevant and valid information to their inquiries.⁴⁹

24. The Committees submit that the Australian Government would be able to protect Australians' democratic rights more adequately if the powers of the AEC were expanded to provide authority to compel social media companies to provide information within specified timeframes. Failure to comply with these requests should be met with substantial penalties.
25. The Committees recommend that the Australian Government could also benefit from modernising legislation that governs the campaigning laws for elections. The Committees submit that the *Broadcasting Services Act 1992* (Cth) is a legislative instrument which could be modernised to include social media and online advertising in relation to the blackout periods.
26. The EU has been particularly proactive in its approach to mitigate foreign interference, by implementing a specialist regulatory body, risk management policies and alert systems. The EU has established a task force as part of their specialist regulatory body known as the EU External Action Services (**EEAS**)⁵⁰, with the intent to investigate and expose misinformation. To date, this task force has been successful in exposing over 65,000 cases of misinformation.⁵¹ These cases are accessible online to assist in increasing the public's awareness.⁵²
27. The Committees submit that the Australian Government should evaluate the current structure and expand the objectives of the Electoral Integrity Assurance Taskforce (**EIA Taskforce**) to take a more proactive approach in exposing cases of interference.
28. The Committees submit that the EIA Taskforce should implement an online searchable platform where previous cases can be listed in plain English to assist with public awareness.
29. Finally, the Committees refer to the developments in Ukraine, where the Ukraine has adopted a 'Learn to Discern' program in its schools to help students identify misinformation in online forums. This

⁴⁹ House of Commons, Digital, Culture, Media and Sport Committee, *Final Report on Disinformation and 'Fake News'*, Recommendations 20-24.

⁵⁰ European Commission, 'Questions and Answers about the East StratCom Task Force' (online, 5 December 2018) <https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en>.

⁵¹ European External Action Service's East Strategic Communication Task Force, 'About', *EUvsDisinfo* (Online) <<https://euvsdisinfo.eu/about/>>.

⁵² *Ibid*.

program is based on the media literacy program offered by IREX, a global education provider.⁵³ The AEC has implemented a 'Stop and Consider' campaign which encouraged voters to check and validate the source of the electoral communication to avoid being misled.⁵⁴ However, currently, there are no in-school programs to equip students on how to identify misinformation.

30. The Committees submit that implementation of school-based programs that educate the next generation of the election processes and how to identify misinformation is instrumental in combating foreign interference through social media. These programs could be introduced to teach students to verify information that is presented in cyber platforms.

Concluding Comments

NSW Young Lawyers, as well as the Communications, Entertainment and Technology Law and International Law Committees, thank you for the opportunity to make this submission. If you have any queries or require further submissions, please contact the undersigned at your convenience.

Contact:



Simon Bruck
President
NSW Young Lawyers
Email: [REDACTED]

Alternate Contact:



Olivia Irvine
Chair
NSW Young Lawyers Communications, Entertainment
and Technology Law Committee
Email: [REDACTED]

Alternate Contact:



Joshua Clarke
Chair
NSW Young Lawyers International Law Committee
Email: [REDACTED]

⁵³ 'Learn to Discern (L2D)- Media Literacy Training', IREX (Web Page) <<https://www.irex.org/project/learn-discern-l2d-media-literacy-training>> .

⁵⁴ 'Stop and Consider', Australian Electoral Commission (Web Page) <<https://www.aec.gov.au/elections/electoral-advertising/files/stop-and-consider-external-flyer.pdf>>.