THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Foreign Interference through Social Media

13 March 2020

Submission to the Select Committee on Foreign Interference through Social Media

Committee Secretary
Department of the Senate
PO Box 6100
Canberra, ACT 2600

foreigninterference.sen@aph.gov.au

Contact: **David Edney**
President, NSW Young Lawyers

Katlyn Kraus
Chair, NSW Young Lawyers International Law Committee

Contributors: Tara Peramatukorn

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

The NSW Young Lawyers International Law Committee **(Committee**) makes the following submission in response to the Senate Inquiry into Foreign Interference through Social Media (**Senate Inquiry**).

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.

The International Law Committee

The International Law Committee (**ILC**) 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 ILC 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 ILC endeavours to broaden the knowledge of international law within the legal profession and the Australian legal system. In doing so, the ILC seeks to promote informed discussion amongst its members and the wider legal community on international law in Australia.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Summary of Recommendations

The Committee makes the following recommendations to the Select Committee on Foreign Interference through Social Media.

1. the Inquiry focus on three pillars of action to combat against foreign interference:
    a. *deterrence* of conduct which would further any form of foreign interference campaign against Australia's political processes and its democracy;
    b. *minimisation* of the spread of misinformation online and through social media platforms; and
    c. *education* of the Australian public on how to detect misinformation;
2. the Australian Government introduce legislation requiring social media platforms to display certain information about advertisements and why they have targeted a particular user;
3. the Australian Government strengthen measures to educate the public on misinformation and how to verify the accuracy of information online;
4. the Australian Government implement a public education program for misinformation online similar to the 'Learn to Discern' program.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Use of social media for purposes that undermine Australia's democracy and values, including the spread of misinformation

Democracy is being threatened around the world.[1] Electoral interference is one of the ways in which foreign actors seek to undermine democracy.[2] Alongside the rising popularity and mainstream usage of social media platforms, foreign interference campaigns which target specific groups and spread misinformation on such platforms has also increased.[3] In the context of foreign electoral interference, this submission defines misinformation as false or misleading information that is disseminated to mislead or deceive its recipients.

Unlike previously non-cyber threats to democracy, threats on social media are subtle but pernicious in their effect.[4] Foreign interference on social media may seek to undermine democracy by increasing fear and inspiring distrust of a target country's political institutions. For example, a study by the Australian Strategic Policy Institute's International Cyber Policy Centre identified three categories of cyber-enabled interference in 97 national elections between 8 November 2016 and 30 April 2019:

(a) interference targeting voting infrastructure and voter turnout;

(b) interference in the information environment around elections; and

(c) long term erosion of public trust in governments, political leadership and public institutions.[5]

The threat to Australia's democracy is no exception. An example to illustrate this includes the social media campaigns waged by Russia online in November 2018. For example, prior to the 2019 Federal Election, Russia is reported to have waged a social media campaign online. Michael Jensen, an Associate Professor at the University of Canberra's Institute for Governance and Policy Analysis, identified that Russia was using Twitter to increase anti-Islamic sentiment and support for Julian Assange in Australia.[6] Foreign interference has the potential to have a direct impact on Australia's future elections, by stoking fears and distrust that could shift targets of social media campaigns into new, more extreme, political identifications or by misinforming voters generally. This danger requires a swift and strong response to foreign interference campaigns to safeguard Australia. This submission makes recommendations as to how the Australian Government may further mitigate the risk posed to Australian democracy.

---

[1] Joint Standing Committee on Electoral Matters, Parliament of Australia, *Australian Electoral Commission Annual Report 2017-18* (Status Report, March 2019) [3.1].
[2] Dhruva Jaishankar, 'The four "I"s undermining democracy', *Brookings* (online, 22 April 2019) <https://www.brookings.edu/blog/order-from-chaos/2019/04/22/the-four-is-undermining-democracy/>.
[3] United States' Department of Homeland Security, *Combatting Targeted Disinformation Campaigns: A whole-of-society issue*, October 2019, 8.
[4] See, e.g. 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>.
[5] Fergus Hanson and Elise Thomas, "Cyber-enabled election interference occurs in one-fifth of democracies", *The Strategist* (online, 17 May 2019) <https://www.aspistrategist.org.au/cyber-enabled-election-interference-occurs-in-one-fifth-of-democracies/>.
[6] 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>.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Responses to mitigate the risk posed to Australia's democracy and values, including by the Australian Government and social media platforms

Responses to mitigate the risks identified include deterrence, minimisation and education.

Deterrence

Foreign Agents

The Australian Government recently implemented measures to deter against conduct performed by or on behalf of a foreign state to promote interference in Australia's political process and democracy. In 2018, the Australian government passed a Bill which added new foreign interference offences in the *Criminal Code*.[7] These offences criminalise conduct which falls short of espionage, but is undertaken by foreign persons seeking to interfere with Australia's political processes, support their own intelligence activities or otherwise undermine Australia's national security.[8] The Commonwealth Director of Public Prosecutions has been allocated $8.5 million in funding to try suspected foreign agents.[9]

The Committee notes that the perpetration of foreign interference involves a wide range of conduct. The new offences are broad enough to capture a wide range of conduct.[10] However, due to fast-paced developments in communications technology, the Committee recommends that the Australian Government frequently assess the adequacy of the legislative deterrence framework to ensure that all relevant conduct is captured.

Social Media Platforms

Facebook maintains a relationship with the Australian Electoral Commission (**AEC**) to monitor political advertisements on its platform. This relationship has not always been productive. For instance, political advertisements are required to display a disclaimer showing who has authorised a political advertisement.[11] In some instances, Facebook has failed to remove political advertisements which have not displayed the required disclaimer in a timely manner.[12] One example is Facebook's removal of an advertisement in breach of this requirement four weeks after being notified by the AEC.[13]

The Australian Electoral Commissioner, Tom Rogers, has previously stated that the AEC has had difficulties with the responsiveness of social media platforms to requests for information about such unauthorised posts.[14]

---

[7] *Criminal Code Act 1995* (Cth) sch 1 div 92.
[8] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (Final Report, June 2018).
[9] Paul Maley, 'ASIO unit gears up to tackle foreign interference', *The Australian* (online, 3 April 2019) <https://www.theaustralian.com.au/nation/politics/asio-unit-gears-up-to-tackle-foreign-interference/news-story/038acb103fb5335878af118ca706e6e3>.
[10] *Criminal Code Act 1995* (Cth) sch 1 div 92.
[11] *Commonwealth Electoral Act 1918* (Cth) s 321D.
[12] Joint Standing Committee on Electoral Matters, Parliament of Australia, *Australian Electoral Commission Annual Report 2017-18* (Status Report, March 2019) [3.19]-[3.23].
[13] 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>.
[14] Nick Evershed and Paul Karp, 'Australian election: Facebook restricts foreign 'political' ads but resists further transparency', *The Guardian* (Web Page, 5 April 2019)

At present, the AEC does not have any power to direct social media companies to remove posts, but can impose fines for offences under the *Commonwealth Electoral Act 1918* (Cth). To date, the AEC has not imposed any punitive measures against social media companies for contraventions under this Act.

In order to encourage compliance with the AEC's rules, regulations and directions, the Committee recommends that a stricter approach be taken to applying punitive measures available under the *Commonwealth Electoral Act 1918* (Cth).

Minimisation

In addition to deterrence, efforts to combat foreign interference will be more effective if minimisation measures are also included. This is because any realistic efforts should account for the fact that it will be near impossible to prevent all forms of foreign interference, particularly as many forms of interference on social media are subtle in nature and difficult to detect immediately.

Australian Government

(i) Intelligence Agencies

The Australian government has significantly bolstered its intelligence capabilities to prevent, detect and minimise foreign interference threats.

On 2 December 2019, the Prime Minister's Office published a media release which committed $87.8 million to setting up a new Counter Foreign Interference Taskforce to strengthen Australia's ability to discover, track and disrupt foreign interference threats.[15] The Taskforce will focus on arrests and prosecutions to enforce the new foreign interference offences introduced in 2018. A Foreign Interference Threat Assessment Centre was also set up, to be jointly operated by the Australian Federal Police and ASIO.

(ii) Australian Electoral Commission

Since April 2019, the AEC has implemented a number of measures to ensure the protection of Australia's elections from foreign influence. These measures include:

(a) setting up an Electoral Integrity Assurance Taskforce to provide the AEC with technical advice and expertise in relation to cyber interference with electoral processes;

(b) implementing a Foreign Influence Transparency Scheme which requires individuals to register under the scheme where they are undertaking a registrable activity undertaken on behalf of a foreign principal for political or government influence purposes; and

(c) working closely with the Australian Signals Directorate and the Australian Cyber Security Centre to ensure the cybersecurity of Australia's electoral systems.[16]

<https://www.theguardian.com/technology/2019/apr/05/australian-election-facebook-restricts-foreign-political-ads-but-resists-further-transparency>.

[15] Prime Minister of Australia, 'Stepping up Australia's Response against Foreign Interference' (Media Release, 2 December 2019).

[16] 'Electoral integrity: 2019 federal election', *Australian Electoral Commission* (Web Page) <https://www.aec.gov.au/elections/electoral-advertising/electoral-integrity.htm>.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Social Media Platforms

The widespread usage of social media platforms to spread misinformation has prompted companies such as Facebook and Twitter to implement their own measures to combat misinformation.

(i) Twitter

Following the 2016 United States' election, Twitter acknowledged that its platform had been "manipulated" as part of Russia's interference campaign.[17] In response, Twitter enacted similar measures to combat foreign electoral interference which applied prior to the 2019 Australian election. These measures included a requirement for accounts running political advertisements to verify their location and identity.[18] Furthermore, Twitter would indicate what material was a considered a political advertisement and display who had paid for them.

Additionally, Twitter has launched an Ads Transparency Center which shows all running advertisements which include promoted tweets, brand reminders, video advertisements and in-stream video advertisements. The Ads Transparency Center is available globally, even to those without a Twitter account, and is updated approximately every 24 hours.[19]

(ii) Facebook

Facebook has implemented some measures to combat the spread of misinformation and inform the public of some key information concerning political advertisements.

In April 2019, Facebook announced that it would be restricting the purchase of political advertisements by foreign entities of an electoral nature during the Australian election campaign period.[20] The restriction took effect from the day after the election was called until the election had concluded. Additionally, Facebook applied a "fact-checking" tool to Facebook posts with articles, pictures or videos. Where material was found to contain false information, the posts would be shown to fewer people but were not removed by the platform.

There were additional transparency features that Facebook did not make available during the Australian election campaign period in April 2019. These features included:

(a) requiring advertisers to pass an approval process before being able to run political advertisements;

(b) requiring advertisements to display a disclaimer showing the name and entity which paid for the advertisement; and

---

[17] Ariel Bogle, 'Twitter rolls out new advertising rules to fight political misinformation', *ABC News* (online, 20 February 2019) <https://www.abc.net.au/news/science/2019-02-20/twitter-new-political-advertising-rules-australian-election/10824944>.
[18] Ibid.
[19] 'Ads Transparency Center FAQs', *Twitter* (Web Page) <https://business.twitter.com/en/help/ads-policies/ads-transparency-center-faqs.html>.
[20] Max Mason, 'Facebook bans foreign-funded political ads during Australian election', *Australian Financial Review* (online, 5 April 2019) <https://www.afr.com/companies/media-and-marketing/facebook-bans-foreign-funded-political-ads-during-australian-election-20190404-p51ath>.

(c) making political advertisements publicly available in an archive.[21]

From June 2019, these features have been applied globally, including to Australian political advertisements.[22]

Alongside this, Facebook has implemented measures to decrease transparency around political advertising. An example is ProPublica, an independent news organisation, which created a Political Ad Collector (**PAC**) tool.[23] Users were able to add the software onto their web browser and:

(a) access information showing why a user was targeted by a particular political advertisement based on race, gender, religion, or some other "affinity" information; and

(b) view political advertisements on Facebook which were not aimed at their demographic group.

Facebook released a statement that it had disabled the PAC tool because it did not want malicious third parties to scrape the user data harvested by the project.[24] Whilst this may be a legitimate concern, this type of information is already easily accessible online.

The Committee recommends that the Australian Government consider passing legislation which requires Facebook to make this information available to users. An Act containing similar measures was introduced in the United States Congress last year.[25] The Act contains amendments which would require social media platforms with over 50 million visitors per month to maintain a publicly accessible file of all advertisements purchased by an individual or group for more than $500. The file would contain a digital copy of the advertisement, a description of the target audience, the number of views generated, dates and times of publication of the advertisement, the rate charged, and contact information of the purchaser.

The Committee recommends that the Australian Government introduce legislation which requires social media companies to make political advertisements and targeted demographic information available to users.

Education

The Australian Public

The public is the target of foreign interference misinformation campaigns.[26] Any strategy that effectively combats foreign interference needs to implement effective measures to safeguard the public. Deterrence and minimisation of misinformation alone will not be effective, as not all misinformation can be filtered out from

---

[21] 'Ads about social issues, elections or politics', *Facebook* (Web Page) <https://www.facebook.com/business/help/167836590566506?id=288762101909005>.
[22] Nick Evershed and Paul Karp, 'Australian election: Facebook restricts foreign 'political' ads but resists further transparency', *The Guardian* (Web Page, 5 April 2019) <https://www.theguardian.com/technology/2019/apr/05/australian-election-facebook-restricts-foreign-political-ads-but-resists-further-transparency>.
[23] 'Political Ad Collector', *ProPublica* (Web Page) <https://projects.propublica.org/political-ad-collector/>.
[24] Jeremy B Merrill and Ariana Tobin, 'Facebook Moves to Block Ad Transparency Tools – Including Ours', *ProPublica* (Web Page, 28 January 2019) <https://www.propublica.org/article/facebook-blocks-ad-transparency-tools>.
[25] Honest Ads Act, S 1356, 116th Congress (2019).
[26] See, e.g. United States' Department of Homeland Security, *Combatting Targeted Disinformation Campaigns: A whole-of-society issue*, October 2019, 6.

public discourse without censoring free speech.[27] Consequently, education is an essential pillar of an effective strategy.

The AEC has run a "stop and consider" campaign to educate voters about how to check the accuracy of information online.[28] It was designed to coincide with the federal election in May 2019 to educate the public on how to check the source of information in relation to the election. The Committee considers this initiative to be a good starting point in a public awareness campaign about misinformation.

The Committee recommends:

1. the Inquiry focus on three pillars of action to combat against foreign interference:
    a. *deterrence* of conduct which would further any form of foreign interference campaign against Australia's political processes and its democracy;
    b. *minimisation* of the spread of misinformation online and through social media platforms; and
    c. *education* of the Australian public on how to detect misinformation;
2. the Australian Government introduce legislation requiring social media platforms to display certain information about advertisements and why they have targeted a particular user; and
3. the Australian Government implement additional measures to educate the public on the existence of misinformation, and how to verify information accuracy and detect misinformation online, not limited to the periods immediately prior to elections.

International policy responses to cyber-enabled foreign interference and misinformation

The issue of foreign interference through social media is not an isolated concern for Australia. Misinformation has proliferated on the internet and has consequently has global impact. Other countries, and groups of nations, have legislated or introduced government programs that Australia could adapt and use to further strengthen existing measures against foreign interference.

European Union

On 5 December 2018, the European Commission published an "Action Plan against Disinformation".[29] The Action Plan acknowledges that social media platforms will play a key role in combating misinformation. This role has already borne some initiatives, including a Code of Practice agreed with social media platforms and the advertising industry in September 2018 to increase online transparency prior to the 2019 European Parliament elections.

---

[27] Darrell M West, 'How to combat fake news and disinformation', *Brookings* (online, 18 December 2017) <https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/ >.
[28] 'Stop and Consider', *Australian Electoral Commission* (Web Page) <https://www.aec.gov.au/elections/electoral-advertising/stopandconsider.htm>.
[29] European Commission, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation*, 5 December 2018, 5.

The Action Plan is based on four key pillars:

(a) improving the capabilities of Union institutions to detect, analyse and expose disinformation;

(b) strengthening coordinated and joint responses to disinformation;

(c) mobilising the private sector to tackle disinformation; and

(d) raising awareness and improving societal resilience.

Australia's existing measures largely target the key pillars above. Australia has already built upon its national security capabilities against foreign interference, including setting up specific bodies to deal with foreign interference threats and working with social media companies to tackle misinformation issues. However, given the key role played by social media platforms in passively assisting foreign interference campaigns, additional measures in line with the Committee's recommendations above are required.

Ukraine

Ukraine has long been subjected to propaganda and misinformation campaigns by Russia, which has sought to delegitimise Ukraine's government since the 2014 Ukrainian revolution. In an effort to counteract these persistent campaigns, in 2015, Ukraine has implemented a "Learn to Discern" program in its schools to help students better identify misinformation and propaganda. The program is based on a media literacy program offered by IREX, a global development and education organisation.[30]

The program teaches critical thinking skills which focus on how to consume information over rather than what to consume. An IREX study of Ukrainian students in Year 8 and 9 who had participated in the program found that students were twice as likely to detect hate speech, and 18% better at identifying misinformation than students that did not participate in the program.[31] The Learn to Discern campaign has been so successful that it has been adapted in other countries such as the United States, Jordan and Indonesia.

The Committee recommends that the Inquiry consider the content in the Learn to Discern program and how it may be adapted to educate the Australian public to identify misinformation.

The Committee recommends:

4. the Australian Government implement a public education program for misinformation online similar to the 'Learn to Discern' program.

---

[30] 'Learn to Discern (L2D) – Media Literacy Training', *IREX* (Web Page) <https://www.irex.org/project/learn-discern-l2d-media-literacy-training>.
[31] Sasha Ingber, 'Students in Ukraine Learn How to Spot Fake Stories, Propaganda and Hate Speech', *NPR* (online, 22 March 2019) <https://www.npr.org/2019/03/22/705809811/students-in-ukraine-learn-how-to-spot-fake-stories-propaganda-and-hate-speech>.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Concluding Comments

NSW Young Lawyers and the Committee 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:

David Edney
President
NSW Young Lawyers

Alternate Contact:

Katlyn Kraus
Chair
NSW Young Lawyers International Law Committee