3 April 2020

Committee Secretary
Department of the Senate
PO Box 6100
Canberra ACT 2600
By email: foreigninterference.sen@aph.gov.au

Re: Foreign Interference through Social Media

About us

The Allens Hub for Technology, Law and Innovation ('the Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information can be found at http://www.allenshub.unsw.edu.au/.

The Datafication and Automation of Human Life is a research program of scholars with the School of Law at Queensland University of Technology. It is dedicated to incubating serious thinking about how data, digital, and automated systems are challenging social, cultural and legal expectations. More information can be found at https://research.qut.edu.au/daaohl/.

The Society on Social Implications of Technology is a technical society within IEEE, a 420,000-member global association of professionals engaged with technology, founded in 1884. SSIT has members in 80 countries and engages in publication, research, education, development of technical standards, and informing public policy development in the field of technology and society. The Australian chapter, which contributed to this submission, was established in 2005. More information can be found at https://technologyandsociety.org/.

All views expressed in this submission are those of the authors and do not represent an institutional position.

Focus and recommendations

We believe that the challenges presented by foreign interference in elections cannot be addressed without considering broader reforms, including:

- Reform of Australia's data protection laws, including the *Privacy Act 1988* (Cth)
- Curriculum reform, that ensures students are better prepared, as citizens and consumers, to navigate a world where others seek to manipulate their behaviour and target their consumption by exploiting their data
- Clarification of Australia's public position on how international law governs state conduct in cyberspace in relation to foreign interference activities.

A complex problem beyond foreign interference

A significant concern about digital platforms is how they have changed political campaigning and elections. This is not solely a question of foreign interference, but rather foreign interference being tied in with at least six other threads.

1. That Australian privacy legislation is based on a consent model rather than a human rights or protection model. Poor data practices have enabled the collection of personal information about large numbers of people, as highlighted in the Cambridge Analytica scandal.[1]
2. The emergence of machine learning, which facilitates data-driven inferencing about likely political opinion and emotional triggers. This means that with a sufficiently large pool of data, it is possible to profile the voting population and deduce means of influence. Machine learning also influences what we see online — many search engines tailor results to users' profiles. Profiling, combined with social networks, creates social media feeds that expose users to views they already believe or are inclined to believe.
3. The ease with which voters can be manipulated by online material.[2] This gives digital platforms an enormous ability to influence citizen participation and choices in elections. For example, in the 2010 US midterm election, Facebook used different 'Today is Election Day' posts that had a large impact on who voted in the election. These nudges are not transparent. Each user knows what they see on Facebook, but no individual is privileged to see the underlying algorithm driving what others are seeing.
4. The use of 'bots' to amplify political communications. 'Bots' is a term used to describe automated agents that initiate communication online, typically through social media accounts. Bots may constantly share content from particular accounts, regularly post particular content, or respond to content that meets particular criteria in standard ways. In automating sharing and tagging content, bots are able to amplify the number of people reading a particular post because the number of accounts commenting or sharing content is often relevant in determining visibility of content in individual feeds. Therefore, bots make it seem as if particular viewpoints have more support in a community than what is in fact the case. In the 2016 US election, pro-Trump bots outnumbered pro-Clinton bots by five to one. There are allegations that some of these were created in Russia.[3] Individuals are often unaware of whether the content they read has been created by a human or a bot.[4]
5. How the algorithms that drive content on digital platforms are designed to optimise user engagement with the platform rather than user education or political balance. Platforms know that users tend to be more engaged with a platform when shown more extreme and controversial content. When this is built into an algorithm, it tends to drive people to content

[1] This can be seen in the documentary *The Great Hack*, www.youtube.com/watch?v=iX8GxLP1FHo.
[2] An example is Facebook's study on emotional contagion: Adam DI Kramer et al, Experimental evidence for massive-scale emotional contagion through social networks' (2014) 111(24) PNAS 8788-8790. See also ACCC, Digital Platforms Inquiry Final Report, June 2019, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.
[3] Bence Kollanyi, Philip N Howard and Samuel C Woolley, 'Bots and Automation over Twitter During U.S. Election', Working Paper, Computational Propaganda Research Project, Oxford Internet Institute, 17 November 2016, https://comprop.oii.ox.ac.uk/research/working-papers/bots-and-automation-over-twitter-during-the-u-s-election. See also the US Grand Jury's indictment in United States v Internet Research Agency LLC dated 16 February 2018, 'United States v Internet Research Agency LLC', (The United States District Court for the District of Columbia, 16 February 2018,) <https://www.justice.gov/file/1035477/download>.
[4] OECD, *Online Advertising: Trends, Benefits and Risks for Consumers*, Report No 272, January 2019, 26.

reflecting more extreme versions of their own views.[5] Individuals are also more likely to read and engage with content that aligns with their pre-existing views. Because social media platforms in particular prioritise content generated or liked by friends, it is easy to fall into 'filter bubbles' where a user is only exposed to content that reflects their existing world-views.

6. The implications of targeted information campaigns. According to a report, organised social media manipulation campaigns have taken place in 70 countries in 2019.[6] In a public election campaign, each side can argue against the facts alleged by the other.[7] However, the situation is quite different when campaigning is conducting on digital platforms. Few people understand the operation of the news feed algorithm on platforms such as Facebook. Each user sees a different automatically generated news feed. Users are thus unaware *why* they are seeing a particular article and, for example, whether they are being targeted because of their profile. Because the news media and election regulators do not know what other users are reading on digital platforms, it is difficult to identify and respond to 'fake news' and illegal campaigns. Where information is targeted at a subset of users, those who might counter the argument or correct the facts do not know of the existence of the misinformation in the first place. Further, a political campaign can pretend to take different, inconsistent positions by targeting different users with subtly different party platforms. This is effectively a misrepresentation but, again, one that is hard for others to correct. There is capacity to develop semi-automated processes around information trustworthiness on digital platforms.[8] However these would rely on the user's judgement to heed generated trustworthy ratings.

There are a variety of potential responses to the web weaved by these various threads. California has passed a law requiring that bots reveal their 'artificial identity' when they are used to sell a product or influence a voter.[9] The law is restricted in scope to larger web sites, applications and social networks, and does not create a private right of action. Rather, it is enforceable by the state Attorney-General. The benefits of this law (and any future laws in a similar vein) are controversial, particularly given the impact on free speech.[10]

---

[5]Zeynep Tufecki, 'We're Building a Dystopia Just to Make People Click on Ads', *YouTube*, 17 November 2017, <https://www.youtube.com/embed/iFTWM7HV2UI>.

[6] Samantha Bradshaw and Philip N Howard, 'The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation', Working Paper, Computational Propaganda Research Project, Oxford Internet Institute, 2019.

[7] This is not confined to foreign influence. The *Commonwealth Electoral Act 1918* does not regulate the amount of electoral advertising or the communication channels a candidate or political party may use. Neither does the *Electoral Act* regulate the truth of electoral communications. There is no equivalent, for example, to the prohibition on misleading or deceptive conduct contained in s 18 of the Australian Consumer Law. This has allowed parties such as the Australian United Party to make claims such as that Joseph Lyons, Billy Hughes and even Robert Menzies were 'Australia Party Prime Ministers' without reproach – see https://www.unitedaustraliaparty.org.au/our-prime-ministers/. Misinformation is damaging whether from a local or foreign source.

[8] IEEE Society on Social Implications of Technology is sponsoring a standard within the IEEE Standards Association P7011 – Standard for the Process of Identifying and Rating the Trustworthiness of News Sources https://standards.ieee.org/project/7011.html.

[9] Bolstering Online Transparency Act (B.O.T. Act), SB 1001 introducing Chapter 6 to Part 3 of Division 7 of the Business and Professions Code.

[10] Madeline Lamo and Ryan Calo, 'Regulating Bot Speech' (2019) 66(4) *UCLA Law Review* 988. See also Bruce Schneier, 'Bots Are Destroying Political Discourse As We Know It' 7 January 2020, *The Atlantic*, https://www.theatlantic.com/technology/archive/2020/01/future-politics-bots-drowning-out-humans/604489/.

A better response might be to tackle the first and third threads. The insufficiency of Australia's privacy laws to protect citizens and consumers has been recognised by a range of actors, including the ACCC.[11] It is the large data stores that ultimately provide the opportunity for foreign actors to target and manipulate Australian voters. In addition, the third thread can be tackled through education, as argued by one of us in a report for the NSW Department of Education.[12] In particular, students can learn through experimentation that search results and news feeds are personalised and engage in interdisciplinary conversations about the best way to navigate this as citizens and consumers. It is also suggested that citizens and consumers might 'take back' control of their data from the platforms through formation of collective 'data unions.' If data unions start to emerge, education will be key to ensure that data curation and management are done appropriately.

Grey zones in international law

The problem with international law relating to foreign interference by cyber means (including through digital platforms) is the uncertainty about the exact way in which existing rules apply to state activities in the cyber context (so called 'grey zones' in the law).[13] Of particular relevance is the customary international law principle of non-intervention which prohibits nation states from coercively interfering in the internal or external affairs of nation states. A state's internal affairs includes its choice of political, economic, social, and cultural system. For example, using digital means to alter the results of an election or alter the operation of election systems would violate this principle (at least according to the position adopted by the United Kingdom and which is generally accepted among international lawyers).[14] However, the problem with targeted information campaigns by foreign actors using digital platforms is that these activities do not clearly amount to 'coercion' (depriving another state of its freedom of choice, or compelling a state to act (or not act) in a particular way).[15] In essence, as the law in this area is uncertain, these activities would likely not be regarded as sufficiently 'coercive' to amount to a prohibited intervention. This in turn has implications for the legally permitted responses available to states victim to these activities.

Allens Hub for Technology Law and Innovation	**QUT**	**Other SSIT**
Lyria Bennett Moses	Michael Guihot	Aurelie Jacquet
Rob Nicholls	Kieran Tranter	Greg Adamson
Heejin Kim		Samuli Haataja
		Sean Goltz

[11] ACCC (n 2).
[12] Lyria Bennett Moses, Helping Future Citizens Navigate an Automated, Datafied World, https://education.nsw.gov.au/content/dam/main-education/teaching-and-learning/education-for-a-changing-world/media/documents/Helping-Future-Citizens-Lyria-Bennett-Moses.pdf.
[13] Michael N Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017) 42(2) *The Yale Journal of International Law Online* 1 <https://campuspress.yale.edu/yjil/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf>.
[14] Jeremy Wright, 'Cyber and International Law in the 21st Century', Speech at Chatham House the Royal Institute of International Affairs, London, 23 May 2018, www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
[15] In relation to the Russian interference in the 2016 US election, see Samuli Haataja, *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics* (2019 Routledge) 172-3.