16 February 2023

Select Committee on Foreign Interference through Social Media
By web:
https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_Social_Media/ForeignInterference47

# Submission on foreign interference through social media pursuant to Terms of Reference of 24 November 2022

## About us

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the 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 about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

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/.

The **Deakin University Centre for Cyber Security Research and Innovation** ('CSRI') is a Strategic Research Centre that brings together a multi-disciplinary team of researchers drawn from Deakin's four Faculties. CSRI's research program is focussed on the technology, systems, human, business, legal and policy aspects of Cyber Security, and is committed to achieving translational and transformational research outcomes for industry, business and society. CSRI's research program is advised by senior industry and thought leaders through its Executive Advisory Board for Cyber (EABC) and is funded through national competitive grants and industry. More information about Deakin CSRI can be found at https://www.deakin.edu.au/csri.

## About this Submission

We are grateful for the opportunity to make a submission as a follow up to our submission of 3 April 2020 which is attached to this submission. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

Our main points relate to:

- The need to link this inquiry to other reform initiatives.
- The need to clarify the democratic values underlying disinformation regulation, particularly truth and free speech and the relationship between them.
- Clarification of Australia's public position on how international law governs foreign interference activities by cyber means, particularly on how international law on sovereignty applies in this context.
- The need to manage the complexity of laws applicable to disinformation and bodies responsible for enforcing these laws.
- The importance of enabling courts and civil society to participate in disinformation detection and action.

## Relationship to earlier submission

As our earlier submission explained, minimising the impact of attempts at foreign interference through social media is not a problem that can be resolved in isolation. It requires a holistic approach that enhances protections for Australians' personal information (particularly in the context of creating psychological profiles), improves Australians' understanding and awareness through public education and curriculum reform, and clarifies Australia's position on international law. Our position on those links is unchanged, but the current position on some of them has evolved, as discussed below. In addition, we add two suggestions here, relating to clear policy ownership and allocation of responsibility and enabling courts and civil society to be part of the solution.

## Link to other reform initiatives

There are a variety of intersecting law reform initiatives underway, including the review of the Privacy Act 1988 (Cth), the draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, the ACCC's Digital Platform Services inquiry, the Senate Economic References Committee's Inquiry into the Influence of International Digital Platforms, and the Department of Prime Minister and Cabinet's Positioning Australia as a Leader in Digital Economy Regulation. For the reasons given in our original submission, issues of data protection, personalised analytics and advertising, limited competition for digital platforms, and the undisclosed use of automated tools are all relevant to understanding the problem of foreign interference in social media. It is crucial that policy addressing the problem be considered holistically rather than separately through independent parliamentary and government processes.

Some means for doing this have been proposed by ANU's Tech Design Policy Centre. While we do not agree on that proposal in its entirety, the need for coherent policymaking across different portfolios is essential.

## Clarifying democratic values underlying disinformation regulation

Internationally and within Australia, disinformation regulation is unclear about the underlying democratic values being protected or promoted. In our view, the core values include truth and freedom of expression and political communication.

Disinformation is a problem for a deliberative conception of democracy, but it is not necessarily problematic for a libertarian conception of democracy. In a deliberative conception of democracy, the search for truth and informed, rational debate are guiding values. Disinformation that obscures the search for truth and informed political decision making must be countered because it undermines these key values. However, a libertarian conception of democracy gives primacy to the liberty and autonomy of the individual and the free flow of ideas and information, uninhibited by governmental controls. It does not presuppose the existence of some ascertainable truth and broadly rejects a governmental role in deciding what information is true or false. In this conception, the regulation of disinformation and misinformation may undermine the autonomy and freedom of the individual to choose what information they consume and share. A laissez-faire approach to free speech, furthermore, relies in the capacity of individuals and the marketplace of ideas to determine which "truths" should prevail. We believe that a deliberative conception of democracy that clearly values truthful discourse as part of the freedom of expression provides a more appropriate framework for Australia's disinformation regulation.

For democratic countries, regulating disinformation involves the idea that the need for protection from the harms of disinformation should be balanced against the need to preserve freedom of expression and political communication. Australia has an interest in the protection of the implied freedom of political communication and more broadly, free and open debate on matters relevant to political decision making. Thus, many advocates argue that the mechanisms against disinformation that are the least oppressive on free and open discussion should be prioritised before moving onto more prescriptive mechanisms which may begin to place pressure on free speech interests. However, the idea of balancing the values of truth and free speech can be confusing and provide unclear guidance to regulators. Rather, the law should clearly articulate that disinformation is problematic in the age of social media and that the duty to safeguard truthful discourse from disinformation is a part or a consequence of some conceptions of freedom of speech.

The values underlying the need to protect against disinformation, together with strategies that individual citizens can undertake, should be part of public education campaigns and the school curriculum.

## A clear position on foreign interference under international law

At the United Nations level, States have reached general agreement about the application of public international law to their international cyber activities.[1] Despite this agreement, there continues to be debate about how the law applies, and a number of States (including Australia) have published their official views on how they consider various areas of international law to be applicable in the cyber context.[2] In relation to foreign interference activities, international law on sovereignty and the

[1] United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc A/76/135 (14 July 2021); United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Final Substantive Report' (10 March 2021) <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>.

[2] See 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' UN Doc A/76/136* (13 July 2021).

non-intervention principle are of particular relevance. Sovereignty in this context refers to various rights and obligations that States have over their information and communication technology (ICT) infrastructure and in their ICT related activities internationally.[3] It is important in delineating the boundary between (lawful) cyber espionage activities and (potentially) unlawful cyber activities violating international law. The non-intervention principle in turn prohibits States from coercively interfering in the internal or external affairs of States.[4] There has been some debate about what 'coercion' means in this context, and Australia has adopted a broad approach to determining this under which a State must be 'effectively deprive[d] … of the ability to control, decide upon or govern matters of an inherently sovereign nature.'[5] Similarly, many States, including Australia, have adopted the position that, for example, manipulating the election result by cyber means would constitute a violation of international law on this basis.[6]

While Australia has adopted a sound position on the non-intervention principle, including providing clear examples of situations in which it would consider foreign interference through cyber means to violate the law, Australia has yet to adopt a similar position on how sovereignty applies. The implication of this is that there remains a lack of clarity about Australia's position on whether disruptive but non-coercive cyber activities by other States violate international law (and the approach that should be used to determining this), and whether such activities are considered acceptable or not.[7] These questions continue to be debated with Australia's close allies, including the UK, New Zealand, and Canada who have adopted different positions on this.[8] Therefore, Australia needs to adopt an official position on how it considers international law on sovereignty to apply in the cyber context, the approach it adopts to determining whether a violation has taken place, and examples of situations in which it considers foreign interference activities to constitute violations of sovereignty. The approach adopted by Canada in 2022 provides an example of a detailed statement of how it considers the law should apply, and Canada's approach is both principled and pragmatic.[9] Adopting a position on this is important in signalling to the international community of States what foreign interference activities conducted by cyber means Australia considers acceptable and unacceptable, and contributing to the development of shared understandings about how international law applies in this context.

[3] Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed, Cambridge University Press 2017) 11-13.

[4] ibid 312-325.

[5] Australian Government, *International Cyber and Critical Technology Engagement Strategy, Annex B: Australia's position on how international law applies to State conduct in cyberspace* (2020) <https://www.internationalcybertech.gov.au/our-work/annexes/annex-b>.

[6] ibid.

[7] Michael Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017) 42(2) The Yale Journal of International Law Online 1, 6-7 <https://bpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf>.

[8] For these and other States' positions, see 'Sovereignty' (*Cyber Law Toolkit*) <https://cyberlaw.ccdcoe.org/wiki/Sovereignty>.

[9] Government of Canada, 'International law applicable in cyberspace' (4 April 2022) [10]-[21] <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng>.

## Managing the complexity of legal regulation

The laws relevant to disinformation are scattered in different statutes and there is no single authority coordinating or leading enforcement, hindering the evaluation and improvement of government response. We recommend managing this complexity through greater transparency regarding government efforts.

Current disinformation regulation suffers from complexity. There are many existing laws that are relevant to countering disinformation. Disinformation may constitute acts that violate various laws and trigger the operation of various legal provisions designed to counter the harmful effects of falsehoods on individuals and society. In the United Kingdom, the United States and Australia, domestic legislation on the digital landscape which are potentially relevant to disinformation have developed along siloed issues of concern, namely, children's safety and bullying, data privacy, national security and terrorism, e-commerce and trade, and election integrity.[10] These pre-existing laws, whilst not originally intended for application to foreign interference, may be interpreted to apply to instances of foreign interference and disinformation on social media. Furthermore, older laws that were developed before the internet, for example, the law on defamation, potentially apply to disinformation (see, eg, the Alex Jones case in the US).[11]

To assess the extent of compliance with existing laws and recommend improvements, observers and overseers must be able to ascertain the full range of governmental bodies, policies and laws operating in this area and the exact role of each governmental body. Some of these bodies are the eSafety Commissioner, the ACCC, the ACMA, DFAT's Counter Disinformation Branch, and the Electoral Integrity Assurance Task Force in partnership with the AFP, DFAT and ASIO. However, it is unclear what exactly each governmental body's role is and whether foreign interference on social media falls within each body's scope of concern. Moreover, there is often little information about how much progress these various governmental bodies have made in monitoring or mitigating disinformation. Compounding this complexity, there does not appear to be a single body responsible for coordinating the government's response to the risks posed to democracy online (whether it be through disinformation or other phenomena on social media and the internet more broadly). Nor is there a single point of contact for the public regarding these risks. Rather, there are various avenues of complaint available and bodies responsible. Whilst there is a National Counter Foreign Interference Coordinator which runs the Counter Foreign Interference Diplomatic Strategy which is described as coordinating 'Australia's whole-of-government efforts to respond to acts of foreign interference', it does not coordinate all online risks to democracy more broadly (such as online misinformation or domestic interference on social media).[12]

We need to reduce this complexity and aid improvements to existing laws, greater transparency and clarity regarding the following are needed. The exact roles and responsibilities of Australian governmental bodies tasked with monitoring, responding to and mitigating disinformation, including

[10] See eg, Digital Economy Act 2017 (UK); U.S. SAFE WEB Act of 2006, 15 USC § 45; Security Agency Act of 2018, 6 USC § 651-674. For Australia, sections 38 and 13(2) of the Foreign Influence Transparency Scheme Act 2018 (Cth), sections 317G and 313 of the Telecommunications Act 1997 (Cth), sections 329(1) and 321D of the Commonwealth Electoral Act 1918 (Cth) and equivalent provisions in South Australia and the Australian Capital Territory.

[11] BBC News, "Alex Jones to Pay Extra $473m Damages over 'fake Sandy Hook' Claim - BBC News," BBC News, November 10, 2022, https://www.bbc.com/news/world-us-canada-63592386.

[12] As described on the website of the National Counter Foreign Interference Coordinator at https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-coordinator

foreign interference on social media, should be clarified. Government should track the progress of these bodies to date, how these bodies interact with each other (if at all), and whether there is a centralised coordinating body or leader responsible for coordinating the attempts by these different bodies to monitor and mitigate the effects of disinformation, including foreign interference on social media. Changes should reflect the need for clear allocation of responsibility and policy ownership.

## Enabling courts and civil society to participate in disinformation detection and action

Under the 'code of practice' approach to disinformation, stopping disinformation operations depends on social media platforms' voluntary cooperation with government. Courts and civil society should be enabled to participate in exposing and stopping disinformation operations. We recommend facilitating access to technical methods and tools for detecting and analysing disinformation operations and the use of evidence obtained from such methods and tools in judicial and other legal proceedings against disinformation.

The 'code of practice' approach to disinformation, adopted in Australia as well as in the UK and the EU, relies on digital platforms' voluntary cooperation with government. It reflects the current dependence of society on both government and platforms' good faith and technical capacity to stop disinformation operations that harm Australians. However, it is well known that because of their business model, digital platforms may see the suppression of viral content as contrary to their business interest. Digital platforms materially gain from increased user engagement with platforms, and nothing engages users more than disinformation and misinformation. Involving more actors, such as civil society and the courts or potentially a dedicated regulatory authority on disinformation, would put more pressure on both platforms and government to stop disinformation operations. It would also prevent the appearance of government and platforms acting like "Big Brother", secretively and only selectively cracking down on some disinformation while tolerating others.

Litigation is a potential, but currently inadequate, antidote to disinformation. Litigation removes individuals from their informational bubbles or echo chambers, assign neutral judges or regulators - instead of simply the marketplace of ideas - to render a judgment on the truth or falsity of certain beliefs and compel action by responsible parties.[13] However, litigation has not yet delivered on its potential. For example, criminal prosecution of offenses of foreign interference through social media, while theoretically possible, is often dismissed as practically infeasible given the jurisdictional and evidentiary challenges.[14]

There are technical methods and tools for detecting disinformation operations in platforms. But clarity about the evidentiary value of information obtained from these technical methods and tools is important if they are to be used in judicial or legal proceedings. Rules could be established regarding the admissibility of evidence produced from technical methods or tools in judicial or legal proceedings.[15] Any such rules, however, must consider the fact that technical methods or tools

[13] Michael Gottlieb and Meryl Conant Governski, "Truth Suits: Litigating Against the Viral Spread of Disinformation," Litigation 48, no. 3 (Spring 2022): 18–23.

[14] See, e.g., Law Council of Australia, "Inquiry of the Select Joint Committee on Foreign Interference through Social Media," Submission (Canberra, Australia: Law Council of Australia, March 25, 2020), 12.

[15] Radim Polcak and Frantisek Kasl, "Proportionate Forensics of Disinformation and Manipulation," in Challenging Online Propaganda and Disinformation in the 21st Century, ed. Milos Gregor and Petra Mlejnková (Cham, Switzerland: Springer International Publishing AG, 2021), 167–93.

employ AI or machine learning, and the need to set acceptable standards of accuracy and explainability.[16]

Ironically, the same jurisdictional and evidentiary challenges thought to hinder court action against disinformation are not raised with respect to platforms' use of technical methods to suppress content on their platforms, as the use of such technical methods within this context is entirely governed by platforms themselves.[17] Indeed, the technical capacity to detect and analyse disinformation operations is concentrated in the hands of the platforms and a few specialised research and monitoring bodies because they are used primarily to support platforms' content moderation, not judicial or legal proceedings. Without access to such technical capacity and agreement on the evidentiary value of information obtained from technical methods and tools, civil society could not effectively monitor platform and government action against ongoing or real-time disinformation operations.

We therefore recommend that the law support greater access to technical methods and tools for detecting and analysing disinformation operations by interested parties and their use in judicial and other proceedings against law violations relevant to disinformation.

Yours sincerely,

**Lyria Bennett Moses**

**Samuli Haataja**

**Madeleine Hale**

**Jayson Lamchek**

**Phillipa Stafford**

[16] Australian guidance documents on the use of "expert systems", both rule-based and machine learning systems, for automated assistance in decision-making include Administrative Review Council, "Automated Assistance in Administrative Decision Making: Report to the Attorney-General" (Canberra, Australia: Administrative Review Council, November 2004); Commonwealth Ombudsman, "Automated Decision-Making Better Practice Guide" (Commonwealth Ombudsman, 2019); Department of Industry, Science and Resources, "Australia's AI Ethics Principles," October 5, 2022, https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles.

[17] In the US, recent Republican-backed proposed law regarding amendment of the Communications Decency Act (47 USC § 230) include clauses that require social media platforms to disclose their methods and policies on moderation, content removal and account deletion. See e.g., S.1384 21st Century FREE Speech Act, H.R.3827 Protect Speech Act, S.2228 DISCOURSE Act.




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.