RESPONSIBLE TECHNOLOGY AUSTRALIA

27 March 2020

Policy Submission

Submission to the Select Committee on Foreign Interference through Social Media

To: *Senate Select Committee on Foreign Interference through Social Media*
From: *Responsible Technology Australia*

Responsible Technology Australia (RTA) would like to thank the Senate Select Committee for the opportunity to input on the inquiry into the risk posed to Australia's democracy by foreign interference through social media. We are excited to see that this issue is rapidly gaining salience amongst key decision makers as we believe that we're at a critical juncture to be able to drive action. We look forward to engaging with this Select Committee and the wider Government through this inquiry and beyond, as we push this conversation forward to ensure appropriate and considered legislation that protects Australian institutions, citizens and democracy.

1.0 EXECUTIVE SUMMARY

The focus of this submission is to highlight the central role the digital platforms play in facilitating foreign interference in Australian democracy. Whilst preventing the actions of foreign malicious actors is a difficult task, understanding, regulating and re-designing the platforms they use to facilitate such harms is achievable and critical..

Our recommendations to the Select Committee focus on establishing more public oversight of these digital platforms in order to inform considered regulation. Responsible Technology Australia calls for the:

1) Transparent understanding of how the digital platforms facilitate foreign interference
    a) Research into the potential risks, vulnerabilities and harms of foreign interference
    b) Conduct ongoing and proactive auditing of the algorithms and how they are amplifying specific types of content and specifically assess the potential for the associated advertising platforms (i.e. FB Ad Platform) to be co-opted for manipulation
2) Establishment of an independent oversight body which includes mechanisms for enforcement

2.0 CONTEXT

In order to achieve directed and effective policy, the link between the business models that power the digital platforms and the resultant architecture, which is primed to be exploited by foreign and malicious actors, must be illustrated.

2.1 The Digital Platforms, their Business Models and the Attention Economy

Firstly, it's important to recognise that the business models (primarily in the form of advertising revenue) of digital platforms like Facebook and YouTube are built on the capitalisation of user attention. This 'attention economy' is powered by the unregulated and limitless collection of user's personal data.

Through this, the digital platforms have built intimate and detailed profiles on their users that enables them to be targeted via their interests, their vices, and their vulnerabilities. This information is then used by the platform's algorithms to feed tailored content that is calculated to have the greatest potential of keeping users engaged and on the platform. This content has been shown to lean toward the extreme and sensational, as it is more likely to captivate user attention[1,2].

This manipulation is facilitated by the digital platforms in two ways:

a) Targeted Advertising | The unfettered approach to data collection has amassed history's largest data sets, allowing advertisers to push beyond normal constraints to deliver direct and granular targeting of consumers. This microtargeting often uses key emotional trigger points and personal characteristics to drive outcomes, which malicious actors can easily exploit to sow distrust, fear and polarisation.

b) Algorithmic Curation | As the primary aim of these platforms is to maximise user time spent on them (to increase their advertising revenue potential), the algorithms are incentivised to serve material that is calculated to engage users more. This content tends to be more extremist or sensationalist or untrue - as it has been shown to be more captivating[3,4]. This opens the door for foreign agents to seed inflammatory and sensational content that users engage with out of outrage or support, and is then amplified by the algorithms which see all engagement as warranting amplification - regardless of the nature of the content.

Most importantly, this illustrates that we need to understand and tackle this issue systematically. Too often, policy approaches to this issue have been focussed on content moderation. Whilst the takedown of material that is clearly false, misleading or clearly intended to divide and misinform is important, these policy approaches will always leave us playing catch-up. The speed in which content can be distributed and amplified to Australian users (especially the types of content used by foreign actors to spread division, misinformation and hate) means that these types of approaches do not have the adaptivity required.

[1] Vosoughi et al. (2018), 'The spread of true and false news online', *Science* found at https://science.sciencemag.org/content/359/6380/1146
[2] Nicas (2 Feb 2018), 'How YouTube Drives People to the Internet's Darkest Corners', *Wall Street Journal* found at https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478
[3] Nicas (2 Feb 2018), 'How YouTube Drives People to the Internet's Darkest Corners', *Wall Street Journal* found at: https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478
[4] Vosoughi et al. (2018), 'The spread of true and false news online', *Science* found at: https://science.sciencemag.org/content/359/6380/1146

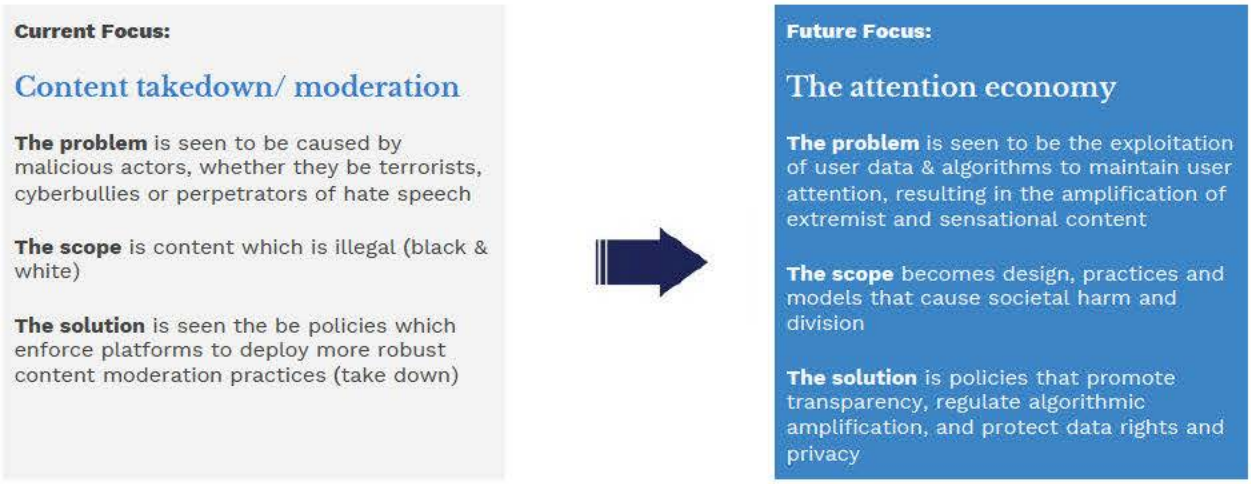

Figure 1: Shift in understanding, focus and scope need to tackle the social harms caused by the digital platforms

2.2 Effects on Democracy

The data collection systems and resultant 'attention economy' that have been set up by the digital platforms leaves us extremely vulnerable to many different forms of manipulation by foreign and malicious actors who wish to threaten the Australian democractic process, exploit our declining trust in our public institutions and generally divide Australian society at large.

The effects of this manipulation have already begun to be seen in Western democracies around the world, weaponising our personal information to drive division and interfere for geopolitical or financial gain. In particular, the capacity for micro-targeting on the digital platforms is completely unprecedented, exacerbating the effect of mis/disinformation whilst also making it much harder to regulate. Additionally, divisive, sensationalist clickbait has been shown to spread faster online, allowing foreign actors to be able to 'game' this system and peddle mass amounts of content with the intention of driving polarisation.

'unlike heritage media, digital and social... can be done in the "dark," so your opponents may not even be aware of the message you are pushing out'.[5]

As clearly documented in the Australian Strategic Policy Institute's Hacking Democracies report[6], the issue of foreign entities utilising the digital platforms to interfere in democracies is pervasive and worldwide.

[5] Hughes (2 May 2019), 'Facebook videos, targeted texts and Clive Palmer memes: how digital advertising is shaping this election campaign', *The Conversation* found at: https://theconversation.com/facebook-videos-targeted-texts-and-clive-palmer-memes-how-digital-advertising-is-shaping-this-election-campaign-115629

[6] Hanson F et al. (2019) 'Hacking Democracies; cataloguing cyber-enabled attacks on elections', *ASPI Policy Brief* found at: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-05/Hacking%20democracies_0.pdf?.RKLLc8uKm1wobfWH1VvC.C88xGWYY29

In particular, two events in 2016:

- the intentional Russian interference in the 2016 US Presidential election, with bought ads designed to exploit division in society for political gain[7,8] and the,
- Cambridge Analytica scandal which leveraged user data to serve curated Brexit messaging[9,10]

thrust this issue from being a fringe theoretical possibility to the primary threat to a functioning democracy and cohesive society. Four years on from this pivotal moment, governments are only just beginning to develop more nuanced and pointed policy approaches to deal with this problem.

Whilst there have been some examples of foreign interference using social media in Australia (as referenced in Figure 2 and our Annex), the full extent of this threat has yet to be comprehensively determined.

This illustrates two key concerns:

1) That we lack the resources, capacity and access to these platforms to fully understand the threats
2) That the examples that have been documented illustrate the vulnerability in which broader segments of Australians would be able to be manipulated

Foreign Interference using Social Media in Australia

A network of Facebook pages run out of the **Balkans profited from the manipulation of Australian public sentiment**. Posts were designed to provoke outrage on hot button issues such as Islam, refugees and political correctness, driving clicks to stolen articles in order to earn revenue from Facebook's ad network[11].

A number of the same accounts Twitter identified as suspected of operating out of the **Russian Internet Research Agency (IRA) targeted Australians** in response to the downing of flight MH17, attempting to cultivate an audience through memes, hashtag games and Aussie cultural references[12].

Figure 2: Two examples of when foreign entities have interfered in Australia

3.0 HOW MIGHT WE RESPOND TO THIS PROBLEM?

Our recommendations on the next steps the Australian Government must pursue centre on two key themes - transparency and independent oversight.

[7] Kelly et al. (22 Aug 2018), 'This is what filter bubbles actually look like', *MIT Media Review* found at: https://www.technologyreview.com/s/611807/this-is-what-filter-bubbles-actually-look-like/
[8] Shane (1 Nov 2017), 'These are the ads Russians bought on Facebook in 2016', *New York Times* found at: https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html
[9] Scott (30 July 2019), 'Cambridge Analytica did work for Brexit groups, says ex-staffer', *Politico* found at: https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/
[10] BBC News (26 July 2018), 'Vote Leave's targeted Brexit ads released by Facebook', https://www.bbc.com/news/uk-politics-44966969
[11] "Facebook trolls and scammers from Kosovo are manipulating Australian users" by Michael Workman, Stephen Hutcheon, ABC News (Mar 16, 2019)
[12] "Russian trolls targeted Australian voters on Twitter via #auspol and #MH17" by Tom Sear, Michael Jensen, The Conversation (Aug 22, 2018)

KEY RECOMMENDATION | TRANSPARENCY

Whilst this Select Committee has taken admirable first steps in uncovering the risks and our vulnerabilities to foreign interference through social media, in order to understand the true extent of this issue, considered and deep research must be undertaken.

Recommendation: Research the potential harm that foreign actors could cause to individuals, society and/or the democractic process in Australia, through the use of the digital platforms

This inquiry should explore several key areas such as;

- Reviewing the potential for social, emotional and political manipulation via digital platforms, including investigating previous and existing international cases (e.g. Brexit) as well as understanding the scale and depth of the data points available for advertisers to use for targeting
- Determining the level of risk Australia faces when advertisers leverage user data to manipulate public sentiment and influence political outcomes, as demonstrated through the Cambridge Analytica scandal
- Reviewing the data sets of Digital Platforms' advertising partners (such as Experian and Quantium) including the data points and customer segments made available to advertisers, as well as the volume of Australians on their lists

How this could be implemented:
A task force would be briefed to conduct an investigation over several months into the potential mechanisms in which the advertising functions on digital platforms could be exploited by malicious actors.

This would require the cooperation of both the digital platforms and advertising partners to identify vulnerabilities, including the extent of data targeting available, the identification verification process for advertisers, the advertising content checks and restrictions, and other procedures set forward by digital platforms and their partners. The outcome of the inquiry would be a set of recommendations for specific platforms to strengthen their advertising systems with the intention of informing future regulation.

Recommendation: Ongoing and proactive auditing of the content that algorithms amplify to users, focusing on the spread of harmful or divisive content that has the potential to influence Australian society and investigate how the digital platform's advertising interface can be co-opted for foreign manipulation.

This would take the form of expanded responsibilities of an independent regulator, which would work to build an evidence base on how algorithms prioritise and distribute certain content and the impact of this on the democratic process in order to inform future regulation. This should focus on (but not be limited to) the following:

- Investigate the nature of algorithmic delivery of content which is deemed to be fake news, propaganda or disinformation
- Audit the extent of algorithmic delivery on the diversity of content to any given user to investigate the impact of ideological filter bubbles
- Audit of the amplification of polarising and extremist political content by these algorithms

How this could be implemented:
Algorithmic audits of these platforms would need to be determined through mandatory collaboration with the relevant companies. This could be set up in a way in which the platforms self-publish a tool

that allows regulators to access what content is being amplified and served in Australia by these algorithms in real-time. This enables regulators to focus on the outcomes of the algorithms rather than the design of the algorithm itself.

This would allow for the mitigation of two key concerns:

1. The inherent sensitivity of allowing external scrutiny of algorithms that are the intellectual property of private enterprises and represent significant trade secrets
2. This would allow regulators to focus on the outcomes of algorithmic curation - as looking at the algorithms' code itself is unlikely to provide insights to the type of content amplified by algorithms.

This mechanism would allow an independent regulator to gather evidence required to assess whether news and other content being recommended by algorithms is in line with societal expectations, and whether actions need to be taken by the platforms to tweak their algorithms to ensure content appropriateness, quality and diversity in line with our media regulation frameworks. An example method to explore modelling algorithmic auditing is available at Algo Transparency, which provides a snapshot of the videos recommended on Youtube.

KEY RECOMMENDATION | INDEPENDENT OVERSIGHT

Recommendation: The Government should undertake a process that explores whether an independent regulator whose role is to evidence and assess the harms of emergent online technologies should be newly created or incorporated into an existing structure/body through an expansion of powers and remits (Office of the eSafety Commissioner, ACCC, ACMA or otherwise).

In order to incorporate many of the above recommendations, there should be strong considerations to consolidate these powers into a fully independent regulator. Whilst there might be natural alignment for this to be housed within the Office of the eSafety Commissioner, due to the pervasive ways that unfettered user data collection and algorithmic amplification affect our society, it can be seen that there are significant overlapping responsibilities with (but not limited to) the ACCC, ACMA, Defence, Australian Intelligence Community, and the Attorney-General's Department. Consolidating responsibility within a centralised and independent body will ensure that coordination and delivery is timely and efficient.

The possibility of the creation of a new entity, adequately equipped, empowered and resourced (most likely through an industry levy that takes into account factors such as size and scope of impact) to deal with the current and evolving harms should be explored. Whilst there are benefits to this approach such as allowing the independent regulator to better consolidate knowledge and learnings across Government portfolios and functions, be properly equipped to liaise with the civil, academic and private sector, and house the necessary technical expertise for governance, research and enforcement. There are also risks, such as the inefficiencies and potential loss of skill in establishing a new Government body, and the lack of clarity in how this new regulator would interact with existing bodies. This needs a proper assessment of how best to enable this regulatory system.

Recommendation: Investigate how the powers of an independent regulator might be expanded to incorporate adequate and proportionate enforcement.

To be effective, a regulator must be able to enforce regulation and go beyond setting transparency reporting expectations. A primary concern with many of the current policy approaches in this space is that they rely on voluntary industry compliance. We believe that in order for Australian democracy to be safeguarded, agreed upon standards must become the normative 'condition of entry' to digital platforms operating within Australia. As such there must be a commitment for the Government to display leadership and enforce these expectations.

Enforcement should incentivise companies to comply whilst providing clear guidelines on how sanctions for non-compliance would be proportionate based on the size of the entity, scale and impact of their potential non-compliance and damage to society.

A wide range of tools could be employed and may include:

- Publishing public notices
- Enforce transparent public reporting
- Issuing provider warnings, reprimands and/or enforcement notices
- Serving civil fines and sanctions

Recommendation: Commit to developing a process that empowers the independent regulator to take action against entities without a legal presence in Australia.

There is an opportunity for the Australian Government to take a world leading role in developing new legal and legislative approaches to adequately deal with the global nature of this issue. It is vital that our independent regulator works with other governments from around the world to coordinate as only an international approach will ultimately be able to mitigate these harms.

What this might look like:

- Setting up multilateral working groups with similar entities internationally
- Adapting a similar concept to the EU's GDPR of having a 'nominated representative' to notionally help enforce compliance

4.0 CONCLUSION

RTA acknowledges the scale of the task ahead to begin to adequately regulate these digital platforms in order to mitigate foreign interference. We look forward to working together to bring about the best outcomes for Australian society.

Should the Select Committee have any questions or require further information, we are happy to engage.

Regards,
Responsible Technology Australia

For any further comment or clarification, please direct enquiries to:

Matthew Nguyen
Director of Policy | Responsible Technology Australia

RESPONSIBLE TECHNOLOGY AUSTRALIA

Annex

AUSTRALIAN EXAMPLES		
Bots stormed Twitter in their thousands during the federal election	2019 - election example - evidence of inauthentic coordinated behaviour during the most recent election - to achieve what means is not clear	A QUT study which examined around 54,000 accounts out of more than 130,000 Twitter users active, during and after the 2019 Australian Federal Election (looking at over 1 million tweets) revealed that 13% of accounts were 'very likely' to be bots, with the majority originating from New York. This is estimated to be more than double the rate of bot accounts in the US presidential election. • This was done through an AI program Botometer - which looks for signs such as tweeting frequently 24 hours a day, tweeting at regular intervals, usernames with lots of numbers and whether their followers also appeared to be bots. • New accounts created during the election campaign were more likely to be bots. • Research into the US election by ANU indicated that the average bot was 2.5 times more influential than the average human. This was measured by their tweets and increased success at attracting exposure via retweets. • Dr Graham said he was still examining the data to see what the Australian bots were tweeting about and whether they were partisan and it was still unknown who created them. • "From a national perspective, the working hypothesis could be that if these are indeed bots, then they're being deployed by interested parties," he said.
Labor asks questions of WeChat over doctored accounts, 'fake news	May 2019 - election - spread of fake news in WeChat - shows potential for special interest groups to manipulate public sentiment to influence	• Labor is losing the battle on influential Chinese social media site WeChat as a wave of fake news posts and doctored accounts target the Shorten campaign on issues such as Safe Schools, taxes and refugee policy. • While many of the posts are unauthorised, making it difficult to know who is responsible for them, one emerged on the weekend containing a doctored tweet purporting to come from Mr Shorten's personal account. The apparent tweet says: "Immigration of people from the Middle East is the future Australia needs." • It was found on multiple WeChat groups posted by Melbourne woman Jing (Jennifer) Li, who has previously identified herself as being a Liberal Party

	electoral outcomes in highly targeted groups	member. Neither Ms Li or the Coalition campaign office responded to questions about the post on Monday. ● Another WeChat account - currently peddling a scare campaign on Labor's economic policies - has been traced back to former Liberal MP Michael Gidley, a member of the party's conservative faction, whose former Victorian state seat of Mount Waverley has high numbers of Chinese-Australian voters. ● The account was registered in Mr Gidley's name in September 2017 before changing in April last year from "MichaelGidleyMP" to "Victoria Brief Talk". In March, four months after Mr Gidley lost his seat to Labor in the state election, it changed again to "Australia Brief Talk". ● The account remains active, with one post falsely claiming that under Labor's new tax policies, retirees whose main income is from share dividends will need to pay an additional $12,850 in taxes each year. It also claims Labor plans big personal tax increases and extra taxes on house sales of $30,000.
Facebook removed 'coordinated inauthentic behaviour' during Australian election	May 2019 - election - Facebook position on Fake news during Aus election	Facebook's position - *"Facebook does not believe that it's an appropriate role for us to be the arbiter of truth over content shared by ordinary Australians or to referee political debates and prevent a politician's speech from reaching its audience and being subject to public debate and scrutiny."* ● It also told the committee it removed 2.2bn fake accounts between January and March 2019, and "the majority of these accounts were caught within minutes of registration". ● Guardian Australia revealed last month the ALP has used its post-election submission to the committee to call for an examination of whether Australian elections are vulnerable to influence by "malinformation" – a term invoked by the Australian Competition and Consumer Commission in its landmark digital platforms review. ● In an interview with Guardian Australia in August, the ACCC chairman, Rod Sims, blasted Facebook's practices, and said the social media giant should have removed the bogus death tax claims given its own independent fact checking processes had found the material to be false.

Facebook videos, targeted texts and Clive Palmer memes: how digital advertising is shaping this election campaign	May 2019 - election - ability of politicians and lobbying groups to spend unchecked	Clive Palmer and United Australia Party + special interest groups • The most recent Nielsen figures put the cost of Palmer's ads since September at around A$30 million, though Palmer says himself he's spent at least A$50 million. • Despite the ubiquity of his ads, though, Palmer is still struggling to connect with most voters. This demonstrates a very important aspect to any advertising campaign: the actual brand still needs to be seen as offering real value to voters. • While not effective, demonstrates the huge amounts that can be spent on the platform unchecked. The increasing influence of lobbying groups • One of the more interesting developments of this election so far is the increasing sophistication, knowledge and strategies of political lobbying groups, or Australia's equivalent to America's PACs. • GetUp! is one such group, collecting A$12.8 million in donations in the last 12 months alone. • The rise of these groups in Australian politics opens a Pandora's Box on just who can influence elections without even standing a single candidate – an issue that's becoming part of politics now in many Western democracies
Scammers from Kosovo manipulating Australian users to profit	2019 - non election, but political - evidence of the types of divisive content that is used to generate engagement on the platform - whether that is for financial or ideological gain	• A network of Facebook pages run out of the Balkans profited from the manipulation of Australian public sentiment. Posts were designed to provoke outrage on hot button issues such as Islam, refugees and political correctness, driving clicks to stolen articles in order to earn revenue from Facebook's ad network. • As the location information only recently became discoverable when Facebook flicked the switch to bring Australia into line with new advertising transparency measures that have been in place in the United States since mid-2018. • The Facebook pages have a combined fanbase of 130,000-plus, which has been built up over several years. The oldest and most popular page, "Australians against Sharia", has been publishing since June 2013. • The "Australians against Sharia" page, which has over 67,000 fans, has also reposted memes attacking Labor Party identities including Bill Shorten, Penny Wong and Julia Gillard, the Greens' Sarah Hanson-Young and the Liberal Party's Julie Bishop.

		• Facebook has now removed these pages, admitting that they violated their policies by engaging in "coordinated inauthentic behaviour" not because of the content • How it works - connected to a news website which hosts various articles. When a post is clicked, the articles are opened in Instant Article - where ads are replaced by facebook ad network and the pages take a cut.
Evidence shows the Internet Research Agency (IRA) targeting Australian politics between 2015 and 2017	2015 and 2017, non-election but political - evidence showing how Russia appear to already be testing different tactics to manipulate the australian public	• Twitter identified 3,841 accounts suspected of operating out of the Internet Research Agency in St Petersburg. A number of these sane same accounts Twitter identified as suspected of operating out of the Russian Internet Research Agency (IRA) targeted Australian politics in response to the downing of flight MH17, attempting to cultivate an audience through memes, hashtag games and Aussie cultural references. • Researchers from Clemson University in the US released 3 million tweets. Analysis of this data set shows how these accounts targeted Australian politics – particularly in reaction to the Australian response to the downing of flight MH17. Some 5,000 tweets mention the terms “#auspol”, “Australia” or “MH17” – with “Australia” the most common of the three. • A jump in activity in Nov 2015 focusing on MH17 correlates with the Australian government’s response to the Russian missile attack on MH17, when Australia deployed fighter aircraft to operate in Syrian airspace where Russian aircraft were also operational. • A second spike in Feb 2017 actually has nothing to do with politics and instead refers to a hashtag game. These Russian accounts encouraged people to come up with Australian names for popular US television programs. While this may seem like innocent fun, it is also a technique of spy craft. “Assets”, in this case, Australian citizens, are recruited on neutral, non-political terms before they are shifted towards political topics.
Chinese media mocks Australia and Prime Minister in WeChat posts	May 2019, election - evidence of anti-liberal propaganda which has the potential to be chinese state interference	Prime Minister Scott Morrison and the Coalition Government have been targeted by online propaganda coming from social media accounts affiliated with the Chinese Communist Party (CCP). Key points: • Propaganda researchers found that there was a clear "anti-Liberal story" coming from social media accounts, many which have close affiliations to the Chinese Government

		• The posts criticise Australia's involvement in the Five Eyes alliance • The researchers say there is little evidence of attacks on Bill Shorten and the Labor Party across their dataset, although this is happening elsewhere on WeChat Data: Across a period of five months from November 2018 to March 2019, the researchers analysed the Australian content on 47 of the most visited WeChat Official accounts in mainland China, 29 of which were aligned with the CCP.
Minister urges scepticism as fake virus news spreads	2020, non election but example of spread of disinformation, which is dangerous in elections	Disinformation around the Coronavirus is spreading online, with posts including claims of how the virus can be caught, suggestions it was deliberately released as well directing people not to consume certain food or visit particular areas in Australia. The rapid spread of disinformation is forcing Facebook and Google to ramp up efforts and use third-party fact-checkers to remove misleading information.
Bushfires, bots and arson claims: Australia flung in the global disinformation spotlight	2020, non election but example of spread of disinformation, which is dangerous in elections	During the Australian bushfire crisis QUT social media analyst Timothy Graham studied 300 twitter accounts to identify any inauthentic behaviour driving the #ArsonEmergency hashtag which was used to push a narrative that the cause of the fires was arson. Many of these accounts were found to be behaving 'suspiciously', compared to other hashtags trending including #AustraliaFire and #BushfireAustralia.
Andrew Forrest, Mike Baird and Waleed Aly caught up in crypto scam	Dec 2019, non election but example of fake news / fake endorsements that the platform do nothing about which could be very damaging in elections	Platforms aren't taking responsibility to the prevent harms and reputational damage they cause Mining magnate Andrew Forrest, former NSW premier Mike Baird and The Project host Waleed Aly were exploited in cryptocurrency scams on Facebook. In an open letter, Forrest called on Zuckerberg to update their regulatory and legislative frameworks to ensure society is protected from the harm Facebook facilitates by allowing scammers to advertise on its platform.
How digital media blur the border	Nov 2018 - non-election, but political, example of	Three prominent WeChat accounts targeted to Chinese diaspora in Australia were shown to dedicate only 0.26% to Chinese politics, compared to 2.85% by SBS in the same time

between Australia and China	how the social platforms opens up whole parts of society to be influenced during elections	period. An absence of political coverage that focuses user attention on gossip and entertainment is known as porous censorship through a "flooding" of the news feed • Data were collected between 1 January 2016 and 1 August 2017. This timeframe includes two Federal government budget speeches, and the 2016 double dissolution election. Given the amount of data, we used a common analytic technique called topic modeling to analyse the content, which categorises stories according to theme. • We found that coverage of terrorism, and crime and justice matters increased on both WeChat and SBS during the data collection period. But when it came to stories about China, the coverage was markedly different. SBS paid far more attention to Chinese politics and Chinese foreign affairs than WeChat accounts – and that disparity has intensified since February 2017. • Comparative findings suggest that the differing content on WeChat and SBS could have markedly different effects on readers. For instance, SBS Mandarin content might serve to give readers a sense of informed civic inclusion and democratic participation in Australian society. On the other hand, the WeChat content might be more likely to emphasise stronger cultural ties to the homeland by creating "distraction and diversion" from sensitive political topics. The near absence of political coverage focuses the attention of WeChat readers on celebrity gossip and other entertainment topics rather than the politics of the People's Republic of China. • This practice has been described as a form of "porous censorship". While readers could seek out information on China from other sources, it takes time and effort to do so. The "flooding" of the daily news feed is effectively more of a tax than a ban on information – especially considering WeChat is a primary source of information for many Chinese living in Australia.
INTERNATIONAL EXAMPLES		
Hacking democracies	Research from 2016 US presidential	Of the 97 national elections in free or partly free countries reviewed for this report during the period from 8 November 2016 to 30 April 2019, **a fifth (20 countries)** showed clear

Cataloguing cyber-enabled attacks on elections **ASPI**	election and the end date was April 2019 - During that period, this research identified 194 national-level elections in 124 countries and an additional 31 referendums.	examples of foreign interference, in several countries with multiple examples. ● There are multiple examples of social media platforms being exploited to reach target populations, often used in concert with state-sponsored media outlets. There is, however, considerable variation in the way social media are exploited. This ranges from organising rallies and amplifying the voices of favoured groups to suppressing voter turnout and exacerbating existing divisions. ○ Might include amplifying a party's existing narrative using social media accounts that have assiduously built up followers over lengthy period ○ it could involve the creation of fake personas who provide inflammatory commentary on divisive issues, as with Luisa Haynes - She was a prolific force in the #BlackLivesMatter community on Twitter. In just over a year, she amassed more than 50,000 followers - —she was fake. ● Foreign interference in the information environment was identified in 10 states: France, Israel, Italy, Malta, the Netherlands, North Macedonia, Spain, Taiwan, Ukraine and the US ● Research identified four alleged actors: Russia (the most dominant by far), China, Iran and the UK.
"Old messages, new memes: Beijing's propaganda playbook on the Hong Kong protests"	Sep 2019 (INTL - Hong Kong) - non-election, political - illustrates potential for foreign actor to deploy online army / mass propaganda tactics against Australia	Digital platforms enabled the Chinese government to run an aggressive propaganda campaign against Hong Kong. The state media endorsed Chinese youth to flood social media pages with patriotic and abusive memes and has supported dueling rallies from Sydney to London. Twitter suspended 936 accounts for "deliberately and specifically attempting to sow political discord" and 200,000 spam accounts linked to the mainland's propaganda campaign. ● The Chinese government has embarked on an aggressive, multipronged propaganda campaign to portray Hong Kong's protesters as extreme, violent and sponsored by foreign actors — using novel tools and approaches. ● Two groups have answered the rallying cry. "Fangirls" are mostly young women who mobilise online in support of their favourite actors and pop idols. In recent weeks, they have come up with a new idol: a-zhong ge, their term of endearment for "handsome older brother China". ● Diba are a nationalistic internet community that goes after individuals they deem to have offended the feelings of the Chinese people, flooding social media pages with patriotic — and often abusive — messages and memes.

		• Overseas mainland Chinese — often students studying abroad — have been encouraged by Chinese state media to support Beijing through counter demonstrations against the Hong Kong protests. • In cities from Sydney to London, a number of these duelling rallies have resulted in clashes but they have still received full-fledged support from Beijing. • Established state outlets have launched social media accounts on which they are encouraged to experiment with more accessible — and sometimes conspiratorial — content. These efforts are paying off. • Controlling the narrative on Hong Kong means the Chinese leadership have had to reach beyond the "Great Firewall", the system Beijing uses to censor the domestic internet and block western media and social media platforms. • State media has paid for its content to be promoted on Twitter, Facebook and YouTube, all of which are barred in China. In July, Beijing's foreign ministry also gave Rmb3.4m to media outlets including the Global Times to monitor and analyse foreign media coverage of China. • Twitter also announced that it had suspended 936 accounts for "deliberately and specifically attempting to sow political discord in Hong Kong" and a further 200,000 spam accounts linked to the mainland's propaganda campaign. YouTube and Facebook took similar actions.
Vote Leave's targeted Brexit ads released by Facebook	INTN (Brexit - 2016) - example of the microtargeting of specific groups, preying on particular vulnerabilities that is hard to detect / limited oversight	The official Vote Leave campaign spent more than £2.7m on targeting ads at specific groups of people on Facebook - helping it to win the 2016 EU referendum. • The US social media giant has now released these ads to a committee of MPs investigating fake news - meaning everyone, not just those they were originally aimed at, can now see them. • The ads, created by Canadian company Aggregate AIQ, often focused on specific issues - such as immigration or animal rights - thought likely to push the buttons of certain groups of people, based on their age, where they lived and other personal data taken from social media and other sources. • The 120 pages of documents appear to back up the findings of the Electoral Commission, which ruled last week that Vote Leave broke electoral law by working jointly with another campaign, BeLeave - something denied by both groups. • There are 1,433 different messages in the data set released by Facebook, all with one common theme - although it is not always clear that they have come from a pro-Brexit campaign.
Russian	INTN (US	• According to two reports commissioned by the

interference in US election (ASPI analysis)	election - 2016) - Russia interference and tactics to sway the election and sow discord	Senate Intelligence Committee, produced by researchers from Oxford University's Computational Propaganda Project and cybersecurity firm New Knowledge, Russian operatives linked to the Internet Research Agency (IRA) specifically targeted African-Americans in the lead-up to the 2016 presidential election in an effort to suppress voter turnout. ● Bret Schafer, a social media analyst and communications officer at the Alliance for Securing Democracy, identified @WokeLuisa—an influential account in the #BlackLivesMatter community—as one of more than 3,000 accounts created by the IRA to target and manipulate the African-American community. Over a 12-month period, the fake @WokeLuisa account 'amassed more than 50,000 followers' and received 'hundreds of thousands of retweets and media coverage in more than two dozen prominent news outlets', enabling the widespread dissemination of disinformation. ● The Oxford University report noted that the Russian operatives posing as Americans online pushed the narrative that 'the best way to advance the cause of the African American community was to boycott the election and focus on other issues instead'. ● Renee DiResta, director of research at New Knowledge, noted that the IRA 'leveraged pre-existing, legitimate grievances wherever they could'. While it's difficult to determine the effect of the IRA's disinformation campaign, the Pew Research Center reported that the voter turnout of African-Americans fell in 2016.