Law Council
OF AUSTRALIA

Inquiry of the Select Joint Committee on Foreign Interference through Social Media

Select Joint Committee on Foreign Interference through Social Media

25 March 2020

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia **3**
Acknowledgement **4**
Introduction **5**
Social media use and Australian democracy **6**
Preliminary matters 6
Uses of social media which may undermine democracy 8
Responses to mitigate risks to Australia's democracy **12**
Existing laws and initiatives to mitigate foreign interference and disinformation 12
Existing strategies by social media platforms 21
Potential options to counter foreign interference and disinformation 24
Compliance with Australian laws **32**
Facebook's compliance with domestic advertising laws 32
International responses to cyber-enabled foreign interference and disinformation **33**
United States 33
Canada 36
United Kingdom 37
France 45
European Union 46

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2020 Executive as at 1 January 2020 are:

- Ms Pauline Wright, President
- Dr Jacoba Brasch QC, President-elect
- Mr Tass Liveris, Treasurer
- Mr Ross Drinnan, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council is grateful for the assistance of its National Criminal Law Committee and National Human Rights Committee in the preparation of this submission. The Law Council is also grateful to the Privacy Law Committee of the Law Council's Business Law Section.

Introduction

1. The Law Council of Australia (**Law Council**) is grateful for the opportunity to provide a submission to the inquiry of the Select Joint Committee on Foreign Interference through Social Media (**Committee**).

2. The Law Council recognises the challenges posed by Australia's security environment. In 2017, the former Director-General of Security, Mr Duncan Lewis categorised espionage and foreign interference as 'an insidious threat' and stated that 'foreign powers are clandestinely seeking to shape the opinions of members of the Australian public, of our media organisations and our government officials in order to advance their country's own political objectives'.[1] More recently, in late 2019, Mr Lewis declared that espionage and foreign interference pose an 'existential threat to Australia' and are 'by far the most serious issue going forward' for Australian security.[2]

3. The impacts of disinformation campaigns on democracy are of global concern.[3] Such campaigns are alleged to have influenced electoral processes in the 2016 United States (**US**) Presidential election and the European Union (**EU**) membership referendum in the United Kingdom (**UK**).[4] The Law Council agrees with the Joint Select Committee on Electoral Matters (**Committee on Electoral Matters**) that, in regard to this threat, 'Australia cannot wait until an electoral crisis occurs, and we should not be complacent or diminish the probability of this threat'.[5]

4. With this changing security environment in front of mind, the Law Council strongly welcomes the establishment of the Committee and the integral work it will undertake over the next two years to consider ways in which to mitigate the serious risks posed to Australia's democracy and values by cyber-enabled foreign interference and disinformation.

5. This is an initial Law Council submission to the Committee's inquiry which responds to each term of reference in turn. The Law Council looks forward to further engagement with this inquiry and welcomes opportunities to consider the key issues and possible responses in more depth in the future.

[1] Evidence to the Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, Canberra, 24 October 2017, 128 (Duncan Lewis) <https://parlinfo.aph.gov.au/parlInfo/download/committees/estimate/420421b5-6149-431f-96e2-06a8423423cf/toc_pdf/Legal%20and%20Constitutional%20Affairs%20Legislation%20Committee_2017_10_24_5667_Official.pdf;fileType=application/pdf#search=%22estimate>.
[2] Duncan Lewis, Address to the Lowy Institute (Speech, Lowy Institute, 4 September 2019).
[3] Joint Standing Committee on Electoral Matters, Parliament of Australia, *Status Report: Australian Electoral Commission Annual Report 2017-18* (March 2019) 1 [1.4] ('*2019 Status Report*').
[4] Ibid 11 [3.15].
[5] Ibid 15 [3.30].

Social media use and Australian democracy

Preliminary matters

Starting point for the Committee's inquiry

6. Digital platforms allow for greater political engagement and debate than ever before. Through the digital sphere creating an unprecedented ability to communicate, the community can better engage with social issues and connect with representatives and others, which enhances and strengthens Australia's democracy.[6] However, the online sphere, marked with the traits of freedom and flexibility, presents new and evolving challenges.[7]

7. The challenges posed by social media to Australia's democracy that are of primary concern to the Committee have been previously identified by the Committee on Electoral Matters in its 2019 status report: that being, cyber-enabled interference by foreign actors in Australia's democratic processes and the impacts of online dissemination of disinformation. It has stated that:

> *Internet communication is posing two interlocked challenges to Australian democracy: hostile strategic actors are attempting to sow division in society by weaponising controversial or misleading information; the self-selection of news and disappearance of attitude-challenging content in some parts of the population's news diet can lead to the rise of 'echo chambers' which facilitate the dissemination of misinformed opinion.*[8]

8. During the Committee on Electoral Matters' review of the 2016 Federal election, the issue of cyber-manipulation of elections, such as the interference of social media bots and foreign interference in electoral events, became an issue of international concern, most notably in the US Presidential election in 2016 and the referendum relating to the UK's membership of the EU.[9] As a result, the Electoral Matters Committee adopted new terms of reference to consider whether cyber-manipulation had any impact on the 2016 election and reported on democracy, disinformation and digital technology in the Australian context.[10]

9. The Electoral Matters Committee resolved that its inquiry into these issues would be continued under a new reference as part of its ongoing oversight inquiry.[11] Consequently, its 2019 Status Report considered: the extent to which social media 'bots' may have targeted Australian voters and political discourse;[12] the likely sources of social media manipulation within Australia and internationally; the ways to address the spread of deliberately false news online during elections; and measures to improve media literacy to Australian voters.[13]

---

[6] Ibid 5 [3.3]; Joint Select Committee on Electoral Matters, Parliament of Australia, *Report on the Conduct of the 2016 Federal Election and Matters Related Thereto* (29 November 2018) 157 [7.1] ('*Report on the Conduct of the 2016 Federal Election*').
[7] Ibid.
[8] Joint Standing Committee on Electoral Matters, *2019 Status Report,* 5 [3.3], citing News and Media Research Centre, Submission No 3.1 to the Joint Standing Committee on Electoral Matters, *Status Report: Australian Electoral Commission Annual Report 2017-18*, 4.
[9] Ibid 7 [1.41].
[10] Ibid 8 [1.43].
[11] Ibid.
[12] See discussion below on page 10.
[13] Joint Standing Committee on Electoral Matters, *2019 Status Report,* xi.

10. The Law Council considers that the findings and recommendations of the Electoral Matters Committee, which are drawn upon throughout this submission, are foundational to the Committee's current inquiry. In identifying that these challenges are worthy of separate, comprehensive review and consideration, the Electoral Matters Committee intended for its recommendations 'to form a basis for future inquiries'.[14]

'Disinformation' rather than 'misinformation' or 'fake news'

11. The Law Council adopts in this submission the term of 'disinformation' rather than 'fake news' or 'misinformation'. This is consistent with the approach of the Electoral Matters Committee, who recommended that all future inquiries into the issues concerning 'fake news' use the term 'disinformation'.[15] It was noted that the EU's Independent High-level Group on Fake News and Online Disinformation (**EU High-level Group on Online Disinformation**) opted for the term 'disinformation' rather than 'fake news' or 'misinformation' in its 2018 report, which has informed the EU's subsequent measures and initiatives on this issue, as is discussed below on page 47.

12. The EU High-level Group on Online Disinformation defined 'disinformation' as:

> *false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit. The risk of harm includes threats to democratic political processes and values, which can specifically target a variety of sectors, such as health, science, education, finance and more. It is driven by the production and promotion of disinformation for economic gains or for political or ideological goals, but can be exacerbated by how different audiences and communities receive, engage, and amplify disinformation.*[16]

13. Whereas, 'misinformation' refers to 'misleading or inaccurate information shared by people who do not recognize it as such'.[17] The EU High-level Group on Online Disinformation avoided the term 'fake news' because, in its view, it has been politicised, as well as for the reason that:

> *The term is inadequate to capture the complex problem of disinformation, which involves content that is not actually or completely 'fake' but fabricated information blended with facts, and practices that go well beyond anything resembling 'news' to include some forms of automated accounts used for astroturfing, networks of fake followers, fabricated or manipulated videos, targeted advertising, organised trolling, visual memes and much more. It can also involve a whole array of digital behaviour that is more about circulation of disinformation than about production of disinformation, spanning from posting, commenting, sharing, tweeting and re-tweeting etc.*[18]

[14] Joint Select Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election*, 159 [7.11].
[15] Ibid 190 [7.94].
[16] Independent High-Level Group on Fake News and Online Disinformation, *A Multi-Dimensional Approach to Disinformation* (Report, March 2018) 10.
[17] Ibid.
[18] Ibid, citing C Wardle and H Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making* (Report to the Council of Europe, 2017) <https://shorensteincenter.org/>.

Uses of social media which may undermine democracy

International examples of foreign interference in democratic processes

14. The US Senate Select Committee on Intelligence found that that 'Russia's targeting of the 2016 US presidential election was part of a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society'.[19] Facebook CEO Mark Zuckerberg has estimated that the Russian-state disinformation agency, the Internet Research Agency, was linked to 470 Facebook accounts in the US, which generated around 80,000 posts over two years which were viewed by approximately 126 million people.[20] On Instagram there were approximately 120,000 pieces of content, reaching approximately an additional 20 million people.[21] Mr Zuckerberg also estimated that the Internet Research Agency spent approximately US$100,000 on more than 3,000 advertisements on both Facebook and Instagram, which were seen by approximately 11 million Americans.[22] The large majority of the material seen by Americans was on socially divisive issues, such as race, immigration, and Second Amendment rights which sought to 'pit Americans against one another and against their government'.[23] Facebook stated that it was 'too slow to spot this type of information operations interference'[24] because, at the time, its security team were aware of, and therefore focused on, traditional foreign cyber threats, such as hacking and malware - it was only after the election that Facebook learnt that:

> *actors had used coordinated networks of fake accounts to interfere in the election: promoting or attacking specific candidates and causes, creating distrust in political institutions, or simply spreading confusion. Some of these bad actors also used our ads tools.*[25]

15. The activities of the Internet Research Agency have been examined by the Oxford Internet Institute together with the US Senate Select Committee on Intelligence.[26] Through studying snapshots of data provided by social media sites, it was discovered that the Russian interference campaign, 'designed to polarize' the US electorate and 'destabilise trust in the media', commenced as early as 2013, with accelerated content production in more recent years across various social media platforms, including Twitter, Facebook, Instagram and YouTube.[27]

16. In the UK, the House of Commons Digital, Culture, Media and Sport Committee's (**UK House of Commons Committee**) 2019 report on *Disinformation and 'Fake News'* found that there is evidence that points to hostile state actors influencing democratic

---

[19] Senate Select Joint Committee on Intelligence, United States of America, *Russian Active Measures: Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media with Additional Views* (Report, Vol 2, 116th Congress, 1st sess, Report 116-XX, March 2019) 5 <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf> ('*Russia's Use of Social Media*').
[20] Evidence to the United State Senate Committee on the Judiciary and the United States Senate Committee on Commerce, Science and Transportation, United States of America, Washington DC, 10 April 2018, 4 (Mark Zuckerberg).
[21] Ibid.
[22] Ibid.
[23] US Senate Select Joint Committee on Intelligence, *Russia's Use of Social Media*, 6.
[24] Facebook, Submission to the United State Senate Committee on the Judiciary and the United States Senate Committee on Commerce, Science and Transportation, United States of America, *Facebook, Social Media Privacy, and the Use and Abuse of Data* (8 June 2018) 109.
[25] Evidence to the United States Senate Committee on the Judiciary and the United States Senate Committee on Commerce, Science and Transportation, United States of America, Washington DC, 10 April 2018, 2 (Mark Zuckerberg).
[26] Phillip N Howard et al, 'The IRA, Social Media and Political Polarization in the United States, 2012-2018' (Report, Computational Propaganda Research Project, 18 December 2018).
[27] Ibid 4-6.

processes.[28] Notably, during the EU referendum campaign, there were a significant number of unique articles published about the referendum from Kremlin-aligned media outlets.[29] Analysis of these articles has identified that the two main outlets were the Russian state-owned news agencies, RT and Sputnik, with 261 articles with a clear anti-EU bias to reporting, reaching 134 million potential impressions: a reach which is significantly broader than the 33 million and 11 million potential impressions from the Vote Leave and Leave.EU websites respectively.[30]

17. As is discussed further below on page 21, Facebook has a policy against 'Coordinated Inauthentic Behaviour' (**CIB**) and regularly removes Pages and accounts which it identifies as engaging in such conduct.[31] For example, in January 2019, Facebook removed 289 Pages and 75 accounts from its site for engaging in CIB[32] that originated in Russia and operated in the Baltics, Central Asia, the Caucasus, and Central and Eastern European countries and which had combined 790,000 followers.[33] Despite representing themselves as independent news or general interest Pages, Facebook reported that these accounts were linked to employees at Sputnik. Some of the Pages posted about topics like anti-NATO sentiment, protest movements and anti-corruption.[34] Approximately $135,000 was spent on ads between October 2013 and January 2019 and around 190 events were hosted by these Pages, the first was for August 2015 and the most recent for January 2019.[35] A further 107 Facebook Pages, Groups, and accounts, as well as 41 Instagram accounts, were removed for engaging in CIB as part of a network that originated in Russia and operated out of Ukraine.[36]

18. The European Commission reported in June 2019 that the evidence collected through its European External Action Service's East Strategic Communication Task Force (**EEAS East Stratcom Task Force**), discussed further below on page 47, identified that there is a 'continued and sustained Russian information campaign which seeks to suppress turnout and influence voter preferences'.[37] It found that malicious actors consistently used disinformation to 'promote extreme views and polarise local debates, including through unfounded attacks on the EU'.[38] It provided the following example:

---

[28] House of Commons Digital, Culture, Media and Sport Committee, Parliament of the United Kingdom, *Disinformation and 'Fake News'* (Final Report, Eighth Report of Session 2017–19, 18 February 2019) 70 [242], citing Cardiff University Crime and Security Research Institute and Centre for Research and Evidence on Security Threats, *Russian Influence and Interference Measures Following the 2017 UK Terrorist Attacks* (Policy Brief, 18 December 2017) <https://crestresearch.ac.uk/resources/russian-influence-uk-terrorist-attacks/> ('*Final Report on Disinformation and 'Fake News'')*; Atlantic Council's Digital Forensic Research Lab, '#Election Watch: Scottish Vote, Pro-Kremlin Trolls', *Medium* (Web page, 13 December 2017) <https://medium.com/dfrlab/electionwatch-scottish-vote-pro-kremlin-trolls-f3cca45045bb>.

[29] House of Commons Digital, Culture, Media and Sport Committee, *Final Report on Disinformation and 'Fake News',* 70 [243].

[30] Ibid.

[31] See, eg, Facebook, 'February 2020 Coordinated Inauthentic Behavior Report', *Facebook Newsroom* (Web page, 2 March 2020) <https://about.fb.com/news/2020/03/february-cib-report/>; Facebook, 'Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar', *Facebook Newsroom* (Web page, 12 February 2020) < https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/>; Facebook, 'Removing Coordinated Inauthentic Behavior From Georgia, Vietnam and the US', *Facebook Newsroom* (Web page, 20 December 2019) <https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/>.

[32] 'Removing Coordinated Inauthentic Behavior from Russia', *Facebook* (Web page, 17 January 2019) <https://about.fb.com/news/2019/01/removing-cib-from-russia/>.

[33] Ibid.

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] European Commission, 'Action Plan Against Disinformation: Report on Progress' (Progress Report, June 2019) 2 <https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf>.

[38] Ibid.

> *Malicious actors have used the fire in the Notre Dame Cathedral to illustrate the alleged decline of Western and Christian values in the EU. They have also been quick to attribute the political crisis and the subsequent collapse of the government in Austria to the 'European deep state', 'German and Spanish Security Services' and individuals.*[39]

19. Foreign interference through social media platforms has not been limited to Facebook. In October 2019, Twitter revealed an archive of 10 million tweets and 2 million photos which had been shared by 3,841 accounts affiliated with the Internet Research Agency and 770 accounts possibly originating from Iran.[40]

Foreign interference in Australia's democratic processes

20. The Electoral Matters Committee reported in its review of the 2016 Federal election that there was no evidence of any cyber manipulation during the 2016 Federal election.[41] During its inquiry, the Committee found little evidence of social media manipulation within Australia, including minimal use of bots.[42]

21. Automated bots are programs capable of generating their own followers that can either be automated or human driven (referred to as 'cyborgs').[43] The UK House of Commons Committee in its *Disinformation and 'Fake News'* report defined bots as:

> *… algorithmically-driven computer programmes designed to carry out specific tasks online, such as analysing and scraping data. Some are created for political purposes, such as automatically posting content, increasing follower numbers, supporting political campaigns, or spreading misinformation and disinformation.*[44]

22. Further, the submissions of Facebook and Twitter reported that there was no interference in Australia's voting or electoral process on their platforms.[45] Regarding the 2019 Federal election, while the inquiry of Electoral Matters Committee is ongoing at the time of writing, research conducted by the News and Media Research Centre found no evidence of a significant, organised operation from foreign actors to support or undermine any of the parties during the 2019 Federal election campaign period.[46]

23. Nonetheless, the Electoral Matters Committee has recommended that, in light of recent international incidents, this issue should continue to be monitored, particularly during election periods.[47] The Law Council agrees: digital technology has significantly

---

[39] Ibid.
[40] 'Enabling Further Research of Information Operations on Twitter', *Twitter* (Web page, 17 October 2018) <https://blog.twitter.com/official/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html>.
[41] Joint Select Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election*, 159 [7.11].
[42] Ibid 180 [7.95].
[43] Ibid 168 [7.40].
[44] House of Commons Digital, Culture, Media and Sport Committee, *Final Report on Disinformation and 'Fake News',* 19.
[45] Facebook, Submission No 224 to the Joint Select Committee on Electoral Matters, Parliament of Australia, *Inquiry into and Report on the 2016 Federal Election and Matters Related Thereto* (8 August 2018); Twitter, Submission No 228 to the Joint Select Committee on Electoral Matters, Parliament of Australia, *Inquiry into and Report on the 2016 Federal Election and Matters Related Thereto* (31 August 2018).
[46] News and Media Research Centre, Submission No 75 to the Joint Standing Committee on Electoral Matters, *Inquiry into and Report on All Aspects of the Conduct of the 2019 Federal Election and Matters Related Thereto* (2019) 13.
[47] Joint Select Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election*, 180 [7.95].

increased the likelihood of foreign interference and, in consideration of international events, Australia should not be complacent about the threat posed.

24. This is particularly important as studies indicate that almost a fifth of all Australians rely on social media platforms for news consumption, with almost a half of Gen Z and a third of Gen Y indicating their main gateway to news is through social media.[48] Research has indicated that Australians are generally concerned about the prevalence of disinformation and discerning fact from fiction online.[49]

25. Further, the research on Australian elections indicates that while there have not been organised information interference operations, this does not necessarily mean that there is no political interference.[50] Research has revealed, for example, that there are:

> *ongoing efforts to influence Australians to adopt more favourable attitudes on specific topics for Beijing. This has included Australian participation in the Belt and Road Initiative, as well as changing its policy stance regarding the participation of Huawei in 5G technologies.*[51]

26. In the conversation about the threats posed by disinformation, the Law Council considers it critical to also note the challenges of disinformation from all sources to democratic processes, not just foreign. The Electoral Matters Committee reported the view of the News and Media Research Centre that 'the threat to Australia of social media manipulation, spread of fake news, and the use of bots appears to currently be more of a domestic threat than one of foreign interference'.[52] Back in January 2018, in an article by Facebook on social media and its impact on democracy, it was noted that foreign interference isn't the only mean of corrupting a democracy.[53] In explaining the global issue of disinformation and fake news, Facebook pointed directly to an Australian example, noting:

> *In Australia, a false news story claimed that the first Muslim woman to be a Member of Parliament has refused to lay a wreath on a national day of remembrance. This led people to flood her Facebook Page with abusive comments.*[54]

Data analytics for political microtargeting purposes

27. Microtargeting is used in a strategy called 'dark advertising', which allows for specific individuals or groups to be targeted, based on the analysis of the data collected about them, with the goal of shifting their opinions, which is only seen by the intended recipient.[55]

28. The significant implications of political advertising via microtargeting, used to better target political advertisements, came to light when the political consulting firm

[48] News and Media Research Centre, Submission No 75 to the Joint Standing Committee on Electoral Matters, *Inquiry into and Report on All Aspects of the Conduct of the 2019 Federal Election and Matters Related Thereto* (2019) 4.
[49] Ibid 5.
[50] Evidence to Joint Select Committee on Electoral Matters, Parliament of Australia, Canberra, 26 February 2020, 3 (Dr Jensen).
[51] Ibid.
[52] News and Media Research Council, Submission No 222 to the Joint Standing Committee on Electoral Matters
[53] Samidh Chakrabarti, 'Hard Questions: What Effect Does Social Media Have on Democracy?' *Facebook Newsroom* (Blog Post, 22 January 2019) <https://about.fb.com/news/2018/01/effect-social-media-democracy/>.
[54] Ibid.
[55] Joint Select Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election*, 176 [7.74].

Cambridge Analytica was linked to a major privacy breach, involving the harvesting of an estimated 87 million Facebook users' personal data.[56] Misuse of this data has been linked to campaigns for the 2016 US Presidential election and the 2016 UK referendum to leave the EU.[57] The details of the Cambridge Analytica-Facebook case are discussed further on page 38, as well as on page 18 regarding Australia's recent action against Facebook in this regard.[58]

Responses to mitigate risks to Australia's democracy

Existing laws and initiatives to mitigate foreign interference and disinformation

Foreign interference laws

29. The foreign interference provisions in the *Criminal Code Act 1995* (Cth) (**Criminal Code**) and the *Foreign Influence Transparency Scheme Act 2018* (Cth) (**FITS Act**) both have a potential role in addressing foreign interference during Australia's democratic or government processes. According to the Electoral Matters Committee:

> *the apparent legislative gap is in domestic and commercial communications, suggesting that further consideration of spam laws, privacy laws, advertising laws and regulatory guidelines is required.*[59]

Foreign interference in the *Criminal Code Act 1995* (Cth)

30. The *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (**EFI Act**) amended the Criminal Code to introduce Division 92 into Part 5.2 of the Criminal Code which contains several new offences relating to foreign interference. The Explanatory Memorandum to the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (Cth) (**EFI Bill**) stated:

> *Foreign interference offences will criminalise conduct engaged in on behalf of a foreign principal that is covert or involves deception, threats or menaces and which seeks to influence a political or governmental process of an Australian government or the exercise of an Australian democratic or political right. Reference to the exercise of Australian democratic or political rights is intended to cover a broad range of rights held by Australians in relation to participation in Australia's democracy, including voting in elections and referenda and participating in lawful protests, rights which clearly fall within the scope of Articles 19, 21, 22 and 25.*[60]

31. The Law Council has previously noted concerns with certain aspects of the foreign interference offences introduced by the EFI Act. In particular, the Law Council was concerned that, in rare circumstances of investigative journalism on behalf of a foreign principal, there should be a defence available for a person acting in the public interest for the foreign interference offences. Other issues previously raised by the Law Council

---

[56] Ibid 174-5 [7.68].
[57] See Information Commissioner's Office, *Investigation into the Use of Data Analytics in Political Campaigns* (Report, 6 November 2018) <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>;
[58] Office of the Australian Information Commission, 'Commissioner Launches Federal Court Action Against Facebook' (Media Release, 9 March 2020) <https://www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook>.
[59] Joint Select Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election*, 157 [7.1].
[60] Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 [27].

concerned issues relating to the definition of the terms 'national security' and 'foreign intelligence agency' as used in the EFI Act.[61]

32. However, the Law Council notes that the offences within Division 92 of the Criminal Code relating to 'intentional foreign interference' are relevant to the current inquiry and were designed to apply to a person who seeks to influence the Australian democratic process in collaboration with, or on behalf of a foreign principal. As was identified in the Explanatory Memorandum to the EFI Bill:

> *Foreign interference can erode Australia's sovereignty by diminishing public confidence in the integrity of Australia's political and government institutions, and undermining Australian societal values. During elections, referendums and plebiscites in particular, foreign interference can undermine the legitimacy or perceived legitimacy of government and its processes, enable the perception of corruption, and obfuscate information that might impact the voting decisions of the public.*[62]

33. It was in order to address these legitimate concerns that the offences relating to foreign interference were included in the Criminal Code. The elements of the offence under section 92.2 that could be relied on in the context of foreign interference through foreign media are that:

    (a) a person engages in conduct on behalf of, or in collaboration with, a foreign principal or a person acting on behalf of a foreign principal or directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal; and

    (b) the person intends that the conduct will either:

        (i) influence a political or governmental process of the Commonwealth or State or Territory; or

        (ii) influence the exercise (whether or not in Australia) of an Australian democratic or political right or duty; and

        (iii) any part of the conduct is covert or involved deception.

34. The offence of 'intentional foreign interference' under section 92.2 of the Criminal Code attracts a maximum penalty of 20 years imprisonment. There is also a specific offence where the person intends that the conduct will influence a specific other person, referred to in paragraph 92.2(2)(c) as 'the target'.

35. The offence under section 92.3 of the Criminal Code of 'reckless foreign interference' is similar to the offence under section 92.2 except the fault element is 'recklessness' rather than 'intention' and attracts a maximum penalty of 15 years imprisonment. It is also an offence to prepare for a foreign interference offence.[63]

---

[61] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018) <https://www.lawcouncil.asn.au/docs/10bff746-c300-e811-93fb-005056be13b5/3390%20-%20National%20Security%20Legislation%20Amendment%20Espionage%20and%20Foreign%20Interference%20Bill%202017.pdf>.
[62] Ibid [28].
[63] *Criminal Code Act 1995* (Cth) s 92.4.

36. For the purpose of the offences in Division 92 the person does not need to have in mind a particular foreign principal and the person may also 'have in mind more than one foreign principal'.[64]

37. However, the Law Council questions the utility of these offence provisions as being capable of being widely used against instances of foreign interference through social media, given the challenges that exist in relation to successfully investigating and prosecuting persons who commit this offence when the 'conduct' occurs outside Australia.

38. The practical challenges of enforcing these offences where the conduct may occur wholly outside Australia are problematic, notwithstanding that section 92.6 provides that the extended jurisdiction within the meaning of Category B of section 15.2 applies to an offence of foreign interference within Subdivision B of Division 92. This provision, providing for 'extended geographical jurisdiction', allows for prosecution of a foreign interference offence where the conduct constituting the alleged offence occurs wholly outside Australia and a 'result of the conduct occurs wholly or partly in Australia'.[65]

39. The Law Council maintains there is still value in retaining the offences in the Criminal Code relating to foreign interference as they provide a symbolic statement concerning the expectations of the conduct of people within or outside of Australia seeking to influence Australian democratic processes. Such measures also serve to express the moral denunciation of the Australian people, through the laws passed by Parliament, of attempts to influence the Australian democratic process on behalf of a foreign actor.

40. The offences can potentially apply to persons who utilise various forms of social media to influence the Australian democratic process in a broad sense on behalf of a foreign actor. While the Explanatory Memorandum to the EFI Bill did not refer to the use of social media to commit the offence, it is clear that the intention of the offences introduced by the EFI Act into the Criminal Code could apply to such conduct where the use of social media is the means to exert the influence on behalf of a foreign actor by deceptive or covert means.[66]

41. While the existing criminal offences relating to 'foreign interference' could be amended to specifically address conduct that seeks to manipulate or undermine the integrity of Australia's democratic system of government through the use of social media, such reforms need to be carefully framed in the context of the right to freedom of expression and the constitutionally implied freedom of political communication as discussed in this submission on page 28.

42. Nonetheless, appropriate criminal offences targeting individuals who use social media to exert foreign influence in such a way as to intentionally compromise Australia's democratic process is one tool that can be deployed to combat this conduct. While it may not be a solution in itself to the problem of preventing foreign influence through social media, it may still prove useful in conjunction with a range of other measures discussed throughout this submission.

[64] Ibid s 92.3(3).
[65] Ibid s 15.2(1)(b).
[66] For the purpose of the foreign interference offences 'deception' is defined in section 92.1 of the Criminal Code as an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes: (a) a deception as to the intentions of the person using the deception or any other person; and (b) conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.

Foreign influence transparency scheme

43. The FITS Act forms part of a suite of reforms designed to address concerns regarding undisclosed foreign influence of public opinion and government policy. The purpose of the scheme created by the FITS Act is to promote greater visibility of the nature, level and extent of foreign influence on Australia's government and politics.

44. The FITS Act presently has a limited role in responding to foreign interference through social media. In its current form, the FITS Act imposes disclosure requirements on people and entities who:

    (a) undertake communications activity in Australia on behalf of the foreign principal for the purpose of political or governmental influence; or

    (b) produce information or material on behalf of a foreign principal for the purpose of being communicated or distributed to the public.[67]

45. While it is clear under the definition of 'communications activity' at section 13 of the FITS Act that information distributed via social media will be included, the platforms on which content is shared will generally fall outside of the definition where they are deemed a disseminator, rather than creator of the content.[68]

46. As noted above in relation to the application of the Criminal Code, the FITS Act only addresses foreign influence relating to certain activities undertaken in Australia on behalf of a foreign principal. The use of social media to publish misinformation directly targeting the Australian public without the use of an intermediary in Australia places significant limitations on the effectiveness of the FITS Act in responding to these threats.

Online political advertising laws

Authorised communications and paid ads on 'electoral matter'

47. The *Commonwealth Electoral Act 1918* (Cth) (**the Electoral Act**) and the *Commonwealth Electoral (Authorisation of Voter Communication) Determination 2018* (Cth) (**the Determination**) establish requirements for the 'authoriser' of paid electoral communications to be identified on social media.

48. The *Electoral and Other Legislation Amendment Act 2017* (Cth) extended the requirement for those responsible for political, electoral and referendum communication to identify themselves on all advertising, irrespective of the communication channel, called an 'authorisation'.[69]

49. Under section 321D, social media content requires an authorisation if the communication includes 'electoral matter'[70] that is communicated by or on behalf of a disclosure entity[71] (e.g. a candidate or a political party), or in a paid advertisement on

[67] See *Foreign Influence Transparency Scheme Act 2018* (Cth) ss 13, 38.
[68] Ibid s 13(3).
[69] Explanatory Memorandum, *Electoral and Other Legislation Amendment Act 2017* (Cth) 5 [2].
[70] 'Electoral matter' is defined as a matter communicated or intended to be communicated for the dominant purpose of influencing the way electors vote in an election (a federal election) of a member of the House of Representatives or of Senators for a State or Territory, including by promoting or opposing: (a) a political entity, to the extent that the matter relates to a federal election; or (b) a member of the House of Representatives or a Senator: *Commonwealth Electoral Act 1918* (Cth) s 4AA.
[71] Ibid s 321B definition of 'disclosure entity'.

social media (including communications which all or part of the distribution or production has been paid for).[72] The authorisation particulars must include:

(a) if the person who authorised the communication is an individual, the name of the person and the relevant town or city of the person;

(b) if the communication is authorised by a disclosure entity (e.g. a registered political party) the name of the entity, the relevant town or city of the entity and the name of the natural person within the disclosure entity responsible for giving effect to the authorisation; or

(c) if the communication is authorised by an entity that is not a disclosure entity or a natural person (e.g. a company that is not an associated entity) the name of the entity and the town or city of the entity.[73]

50. The authorisation must appear either at the end of the communication or, if the particulars are too long to be included in the communication, in a website accessible by a URL included in the communication, or in a photo included in the communication.[74]

51. When a social media Page is established by, or on behalf of, a disclosure entity, it must include an authorisation, which can be fulfilled by the authorisation particulars being placed in the 'Bio' or 'About' section of the social media Page.[75] In this instance, it is then unnecessary for every post or tweet on that social media Page to be 'authorised'.[76] However, the Australian Electoral Commission (**AEC**) recommends that, if a video or image which contains 'electoral matter' is posted to a social media Page by, or on behalf of, a disclosure entity, the authorisation should be embedded within that video or image so that authorisation is not lost when the video is reposted or shared.[77] However, this is not required by law.

52. The AEC is responsible for investigating breaches of, inter alia, the authorisation rules and enforcing relevant penalties. Complaints regarding unauthorised electoral communications on social media can be made to the AEC via an online form.[78] The AEC has the right to take any course of action it considers necessary in the circumstances.[79] Further, under section 321F, the AEC has information-gathering powers whereby it can request information or documents from a person if there is reason to believe that the information or document is relevant to assessing compliance with section 321D.

53. In instances where the AEC considers that a communication with 'electoral matter' is not compliant with the authorisation requirements, the AEC writes to the relevant person to request that the communication is withdrawn until such time as the communication is properly authorised to comply with the law.[80] If there is continued non-compliance or a more serious breach of the Electoral Act (see below for further discussion on page 32),

---

[72] Ibid s 321D.
[73] Ibid s 321D(5).
[74] *Commonwealth Electoral (Authorisation of Voter Communication) Determination 2018* (Cth) s 9.
[75] Australian Electoral Commission, 'Electoral Backgrounder: Electoral Communications and Authorisation Requirements' (Web page, 16 July 2019) <https://www.aec.gov.au/About_AEC/Publications/Backgrounders/authorisation.htm>.
[76] Ibid.
[77] Ibid.
[78] Australian Electoral Commission. 'I'd Like to Make a Complaint' (Web page) <https://formupload.aec.gov.au/Form?FormId=complaint>.
[79] Australian Electoral Commission, 'Electoral Backgrounder: Electoral Communications and Authorisation Requirements' (Web page, 16 July 2019) <https://www.aec.gov.au/About_AEC/Publications/Backgrounders/authorisation.htm>.
[80] Ibid.

the AEC may seek an injunction or apply for a civil penalty to be imposed.[81] The penalty for a breach of the authorisation requirements by an individual is up to 120 penalty units and up to 600 penalty units for a body corporate.[82] The example of the AEC undertaking these steps in discussed below on page 32.

Misleading or deceptive electoral advertising

54. Subsection 329(1) of the Electoral Act makes it an offence to print, publish or distribute, or cause, permit, or authorise to be printed, published or distributed, any matter or thing that is likely to mislead or deceive an elector in relation to the casting of a vote. However, the prohibition in section 329 is limited to 'misleading or deceptive conduct which might affect the process of casting a vote rather than the formation of the political judgment about how the vote will be cast'.[83]

Commitments to action from the Digital Platforms Inquiry

55. During 2018 and 2019, the Australian Competition and Consumer Commission (**ACCC**) undertook an inquiry into the impact of digital platforms on consumers, business and news media. The final report, *Digital Platforms Inquiry,* considered the issue of disinformation, and investigated questions such as the role and impact of digital platforms, including issues arising from alleged anti-competitive conduct, privacy concerns, disparity in media regulation, copyright issues harmful online content, the scope and scale of user information collected by platforms, and the risk of exploitation of consumer vulnerabilities.[84]

56. There are several findings and recommendations from the *Digital Platforms Inquiry* which are important when considering the steps being taken to address news quality, disinformation and protecting Australians personal data on social media platforms.

Codes of conduct for digital platforms

57. The ACCC recommended that digital platforms with more than one million monthly active users in Australia implement an industry code of conduct to govern the handling of complaints about disinformation on their services.[85] It was recommended that it should be restricted to complaints about disinformation that meet a 'serious public detriment' threshold. The ACCC recommended that the code should also outline actions that constitute suitable responses to complaints, up to and including the take-down of particularly harmful material.[86]

58. The ACCC suggested that the code should be registered with and enforced by an independent regulator, such as the Australian Communications and Media Authority (**ACMA**), who should:

    (a) be given information-gathering powers enabling it to investigate and respond to systemic contraventions of code requirements;

    (b) be able to impose sufficiently large sanctions to act as an effective deterrent against code breaches;

[81] Ibid.
[82] *Commonwealth Electoral Act 1918* (Cth) s 321D.
[83] *Peebles v Honourable Tony Burke* [2010] FCA 838, [10].
[84] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 1 ('*Final Report of the Digital Platforms Inquiry*').
[85] Ibid 370.
[86] Ibid.

(c) provide frequent public reports on the nature, volume and handling of complaints received by digital platforms about disinformation; and

(d) report annually to Australian Government on the efficacy of the code and compliance by digital platforms.[87]

59. It was also recommended that the code should also consider appropriate responses to 'malinformation', which the *Digital Platforms Inquiry* defined as 'information inappropriately spread by bad-faith actors with the intent to cause harm, particularly to democratic processes'.[88]

60. The ACCC recommend that ACMA should review the code after two years of operation and make recommendations as to whether it should be amended, replaced with an industry standard, or replaced or supplemented with more significant regulation to counter disinformation on digital platforms.[89]

61. In the Australian Government's response to the *Digital Platforms Inquiry,* it committed to asking the major digital platforms to develop a voluntary code of conduct for disinformation and news quality.[90] The Australian Government has stated that the ACMA will have oversight of the development of the code as well as its implementation, including reporting to the Australian Government on the adequacy of platforms' measures and the broader impacts of disinformation.[91] The Australian Government has requested this report be received by no later than June 2021.

62. It is intended that these codes will seek to address the concerns regarding disinformation and credibility signalling for news content and outline the actions that the platform will take to tackle disinformation, as well as initiatives to support Australians to evaluate the quality and credibility of news and information.[92] Learnings from international examples, such as the *European Union Code of Practice on Disinformation* (discussed further on page 48), are intended to guide and inform the development of such codes.[93]

63. The Australian Government has committed to evaluating, through the ACMA's reporting, the effectiveness of the voluntary codes of conduct in 2021,[94] declaring that if the problems of disinformation and online news quality are not being sufficiently mitigated by voluntary measures, it will consider the need for further action.[95]

Action against interferences with privacy

64. The ACCC's *Digital Platforms Inquiry* recommended that the Australian Government develop a binding online privacy code to 'enable proactive and targeted regulation of digital platforms' data practices'.[96] The ACCC intended for the *Digital Platforms Privacy Code* to apply to all digital platforms supplying social media, as well as supplying online

[87] Ibid.
[88] Ibid.
[89] Ibid.
[90] Treasury, Australian Government, *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (2019) 7 <https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf> ('*Government Response to the Digital Platforms Inquiry*').
[91] Ibid.
[92] Ibid.
[93] Ibid.
[94] Ibid.
[95] Ibid 13.
[96] Australian Competition and Consumer Commission, *Final Report of the Digital Platforms Inquiry,* 481, Recommendation 18.

search and content aggregation services to Australian consumers and which meet an objective threshold regarding the collection of Australian consumers' personal information.[97]

65. It recommended that the *Digital Platforms Privacy Code* contain provisions targeting particular issues arising from data practices of digital platforms, such as requirements to:

    (a) provide and maintain multi-layered notices regarding key areas of concern and interest for consumers;

    (b) provide consumers with specific, opt-in controls for any data collection that is for a purpose other than the purpose of supplying the core consumer-facing service;

    (c) give consumers the ability to select global opt-outs or opt-ins, such as collecting personal information for online profiling purposes or sharing of personal information with third parties for targeted advertising purposes;

    (d) additional restrictions on the collection, use or disclosure of children's personal information for targeted advertising or online profiling purposes and requirements to minimise the collection, use and disclosure of children's personal information;

    (e) maintain adequate information security management systems in accordance with accepted international standards; and

    (f) establish a time period for the retention of any personal information collected or obtained that is not required for providing the core consumer-facing service.[98]

66. The Australian Government's response to the *Digital Platforms Inquiry* reaffirmed its commitment, first announced in March 2019, to 'require the development of a binding privacy code that will apply to social media platforms and other online platforms that trade in personal information'.[99] The Office of the Australian Information Commissioner (**OAIC**) has been tasked with the development *Digital Platforms Privacy Code*.

67. The Australian Government considers that greater transparency about data sharing, methods to best practice consent requirements when collecting, using and disclosing personal information, prevention of the use or disclosure of personal information upon request and express rules to protect personal information of children and vulnerable groups are key intended components of the *Digital Platforms Privacy Code.* The Australian Government has committed to releasing draft legislation for consultation, and subsequent to consultation, introduction of legislation and the development of the code in 2020.[100] The Law Council has expressed strong support for the development of the *Digital Platforms Privacy Code*.[101]

68. Additionally, in March 2020, the OAIC lodged proceedings in the Federal Court of Australia against Facebook in relation to the Cambridge Analytica story. It is alleged that the personal information of Australian Facebook users was disclosed to the *This is Your*

[97] Ibid.
[98] Ibid.
[99] Treasury, Australian Government, *Government Response to the Digital Platforms Inquiry*, 5.
[100] Ibid.
[101] Law Council of Australia, Submission to the Australian Competition and Consumer Commission, *Digital Platforms Inquiry – Preliminary Report* (15 February 2019) 12-3; Law Council of Australia, Submission to the Treasury, *Digital Platforms Inquiry* (18 September 2019) 8 [36].

Digital Life app for a purpose other than the purpose for which the information was collected, in breach Australian Privacy Principle 6 in the *Privacy Act 1988* (Cth).[102] The OAIC alleges in the statement of claim that the personal data of around 311,127 Australian Facebook users was sold and used for purposes including political profiling, falling well outside users' expectations, as most of the users did not install the app themselves and the disclosure of their data was triggered through their friends' use of the app.[103] Further, the OAIC also alleges that Facebook did not take reasonable steps during this period to protect its users' personal information from unauthorised disclosure, in breach of Australian Privacy Principle 11.[104] Further details about the facts leading to this case are on page 38.

Measures surrounding the 2019 Federal Election

Foreign political advertising

69. During April and May 2019, Facebook temporarily prohibited political or electoral ads purchased from outside Australia, whereby ads from foreign entities that contained references to politicians, parties or election suppression, or political slogans or party logos, were banned.[105] Facebook stated that this was one measure 'to combat misinformation and foreign interference during the Australian election campaign'.[106] Further actions by Facebook during the 2019 Federal election are discussed below on page 23.

'Stop and Consider' campaign

70. Leading up to the 2019 Federal election, the AEC undertook the 'Stop and Consider' campaign on disinformation. The campaign, which was the first of its kind in Australia, included advertisements on Facebook, Twitter, Instagram and Google that encouraged voting Australians to check the source of the material to avoid being misled by disinformation.[107] The AEC considered this campaign to be successful, with over 55,000 impressions and 40 percent of those who recognised the campaign reporting that they would take action on account of seeing the campaign.[108]

Electoral Integrity Assurance Task Force

71. The Electoral Integrity Assurance Taskforce (**Electoral Integrity Taskforce**) was established for the 2019 Federal election.[109] The Electoral Integrity Taskforce constituted a network of Australian Government agencies to provide advice on a range

[102] *Privacy Act 1988* (Cth) sch 1 pt 3. See Office of the Australian Information Commission, 'Commissioner Launches Federal Court Action Against Facebook' (Media Release, 9 March 2020) <https://www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook>.
[103] Ibid.
[104] *Privacy Act 1988* (Cth) sch 1 pt 4.
[105] Facebook, Submission No 140 to the Joint Select Committee on Electoral Matters, *Inquiry into and Report on All Aspects of the Conduct of the 2019 Federal Election and Matters Related Thereto* (8 October 2019) 5.
[106] Nick Evershed and Paul Karp, 'Australian Election: Facebook Restricts Foreign 'Political' Ads But Resists Further Transparency', *The Guardian* (online, 5 April 2019) <https://www.theguardian.com/technology/2019/apr/05/australian-election-facebook-restricts-foreign-political-ads-but-resists-further-transparency>.
[107] Australian Electoral Commission, Submission No 120 to the Joint Select Committee on Electoral Matters, *Inquiry into and Report on All Aspects of the Conduct of the 2019 Federal Election and Matters Related Thereto* (2018) 32.
[108] Ibid.
[109] Ibid.

of issues for the election.[110] The AEC noted that it observed a 'marked improvement in engagement undertaken with major online and social media platforms'.[111] While the Electoral Integrity Taskforce is not permanent, it has been noted that it will continue to work together on electoral integrity, when required, and options to extend support to state and territory election commissions have been considered.[112]

Existing strategies by social media platforms

Disinformation campaigns or operations

72. Facebook's CIB policy seeks to prevent and stop campaigns that seek to manipulate public debate.[113] This policy states that its objective is to target actors that are using deceptive means to conceal their identity or the organisation behind a campaign, in order to make a campaign appear more a popular or trustworthy than it truly is, or to evade enforcement efforts.[114] Facebook identifies foreign efforts to manipulate public debate in another country as a particular type of CIB, the policy on which is to apply the 'broadest enforcement measures including the removal of every on-platform property connected to the operation itself and the people and organizations behind it' when conducted on behalf of a government entity or by a foreign actor.[115] Monthly CIB reports are published online which include the CIB detected and removed by Facebook.[116]

Transparency in political advertising

Facebook

Ad Library

73. In some jurisdictions, Facebook has implemented two key political advertising transparency measures. The first is the authorisation process for advertisers running ads about social issues, elections or politics.[117] The second is the Ad Library.[118]

74. Advertisers running ads about social issues, elections or politics are required to go through the authorisation process, so that a disclaimer with the name and entity that paid for the ads can be included in the ad. If an advertisement runs without a disclaimer, it can be paused, disapproved and added to the Ad Library, until the advertiser completes the authorisation process.[119]

75. In the countries in which it is live, the Ad Library contains all active ads as well as past ads. For social issues, elections or politics ads, the Ad Library offers additional

[110] This comprised the Australian Electoral Commission, Department of Finance, Department of the Prime Minister and Cabinet, Department of Communications and the Arts, Attorney-General's Department, Department of Home Affairs, Australian Federal Police and Australian Signals Directorate: ibid.
[111] Ibid.
[112] Ibid.
[113] Nathaniel Gleicher, 'How We Respond to Inauthentic Behavior on Our Platforms: Policy Update', *Facebook Newsroom* (Blog post, 21 October 2019) <https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/>.
[114] Ibid.
[115] Ibid.
[116] See, eg, Facebook, 'February 2020 Coordinated Inauthentic Behavior Report', *Facebook Newsroom* (Web page, 2 March 2020) <https://about.fb.com/news/2020/03/february-cib-report/>.
[117] Facebook for Business, 'Be Authorised to Run Ads about Social Issues, Elections or Politics', *Ads About Social Issues, Elections or Politics* (Web page) <https://en-gb.facebook.com/business/help/2405092116183307?id=288762101909005>.
[118] Facebook for Business, 'About the Ad Library', *Ads About Social Issues, Elections or Politics* (Web page) <https://en-gb.facebook.com/business/help/208949576550051?id=288762101909005>.
[119] Ibid.

information including spend, reach and funding entities.[120] It is a general rule that ads are archived for seven years.[121] In some jurisdictions, all ads about social issues, elections or politics will be added to the Ad Library, even if the advertiser who created them hasn't completed the advertisement authorisation process.[122]

76. Advertisements about social issues, elections or politics are classified by Facebook as being:

    (a) made by, on behalf of or about a current or former candidate for public office, a political figure, a political party or advocates for the outcome of an election to public office;

    (b) about any election, referendum or ballot initiative, including 'go out and vote' or election campaigns;

    (c) about social issues in any place where the advertisement is being placed; or

    (d) regulated as political advertising.[123]

77. These transparency tools commenced in the United States and Canada. In April 2018, Facebook announced that it was testing a new feature called 'view ads' in Canada which allowed users to see the advertisements, political or otherwise, that a Page was running.[124] The authorisation processes for political advertising and the Ad Library commenced in the US in May 2018, whereby it started to require advertisers in the US to be authorised before posting advertisements about social issues, elections or politics, as well as to place a 'Paid for by' disclaimer on their advertisements to communicate who is responsible for them,[125] which were then added to the Ad Library for seven years.[126]

78. These tools were extended to the United Kingdom and Brazil in June 2018, to India in February 2019, Israel and Ukraine in March 2019, as well as to the EU members in May 2019. In June 2019, the Ad Library also went live in Singapore, Canada and Argentina, and are now also live in Poland, Sri Lanka and Taiwan.[127] There are slightly different requirements and processes in each jurisdiction for the authorisation process for advertisers.[128] There are also different features, and therefore different functioning, of the Ad Library between jurisdictions.[129] The Ad Library can be explored online through

---

[120] Ibid.
[121] Ibid.
[122] Facebook for Business, 'Be Authorised to Run Ads about Social Issues, Elections or Politics', *Ads About Social Issues, Elections or Politics* (Web page) <https://en-gb.facebook.com/business/help/2405092116183307?id=288762101909005>.
[123] Ibid.
[124] Rob Goldman, 'Making Ads and Pages More Transparent', *Facebook Newsroom* (Blog Post, 6 April 2018) <https://about.fb.com/news/2018/04/transparent-ads-and-pages/>.
[125] Robert Leathern, 'Shining a Light on Ads With Political Content?', *Facebook Newsroom* (Blog Post, 24 May 2018) <https://about.fb.com/news/2018/05/ads-with-political-content/>; Katie Harbath and Sarah Schiff, 'Updates to Ads About Social Issues, Elections or Politics in the US' *Facebook Newsroom* (Blog Post, 28 August 2019) <https://about.fb.com/news/2019/08/updates-to-ads-about-social-issues-elections-or-politics-in-the-us/>.
[126] Facebook for Business, 'About the Ad Library', *Ads About Social Issues, Elections or Politics* (Web page) <https://en-gb.facebook.com/business/help/208949576550051?id=288762101909005>.
[127] Ibid.
[128] See Facebook for Business, 'Be Authorised to Run Ads about Social Issues, Elections or Politics', *Ads About Social Issues, Elections or Politics* (Web page) <https://en-gb.facebook.com/business/help/2405092116183307?id=288762101909005>.
[129] For example, there are differences between jurisdictions regarding when an advertisement will added to the Ad Library (see differences in Brazil to Austria and Argentina), what happens to advertisement when they don't have a disclaimer (see differences in Austria, Argentina, Brazil, Israel, Poland, Singapore and Taiwan to

a web interface and queried by an application programming interface.[130] For each country (except Brazil[131] and Sri Lanka[132]) aggregated data is also published in form of 'reports'.[133]

79. Importantly, it was announced in March 2020 that Facebook will extend the authorisation process for advertisements about social issues, elections or politics in Australia and introduce the Ad Library to Australia.[134]

80. Outside these countries, it is voluntary to go through the advertisement authorisation process for advertisements about social issues, elections or politics, and therefore disclaimers on this type of advertising are optional, unless mandated by domestic laws. Consequently, there is no live Ad Library available for political advertisements outside the jurisdictions noted above.

81. In January 2020, Facebook announced further updates to the Ad Library, which includes showing the estimated target audience size for each political, electoral or social issue advertisement and adding controls to let users choose how an advertiser can reach them with a Custom Audience from a list and to allow users to limit the number of political and social advertisements they see.[135]

Measures surrounding the 2019 Federal election

82. Turning to the Australian context, Facebook noted that its efforts to 'safeguard the 2019 election' included:

    (a) temporary restrictions on foreign political or electoral advertisements;

    (b) expanding the Third-Party Fact Checking program to Australia; and

    (c) working closely with the Australian Government's Election Integrity Taskforce.[136]

Twitter

83. In October 2019, Twitter announced that the platform would no longer allow political advertisements on its platform.[137] 'Political content' is defined as:

Canada, EU, India, Ukraine, United Kingdom, United States) and what happens when the advertiser whose advertisement targets a particular jurisdiction doesn't reside therein (see requirements in Canada, EU, India, Ukraine, United Kingdom and United States): Facebook for Business, 'About the Ad Library', *Ads About Social Issues, Elections or Politics* (Web page) <https://en-gb.facebook.com/business/help/208949576550051?id=288762101909005>.

[130] The API allows a search to perform custom keyword searches of ads stored in the Ad Library.

[131] Ambassador for Digital Affairs, 'Facebook Ads Library Assessment' (Web page) <https://disinfo.quaidorsay.fr/en/facebook-ads-library-assessment>.

[132] Letter from Centre for Policy Alternatives to Mr Senura Abeywardene, Country Representative for Sri Lanka to Facebook, 30 September 2019 <https://www.cpalanka.org/wp-content/uploads/2019/11/Letter-to-Facebook-on-Campaign-Spending.pdf>.

[133] Facebook, 'Ad Library Report' (Web page) <https://www.facebook.com/ads/library/report/>.

[134] Fergus Hunter, 'Facebook Imposes New Transparency Rules on Political Ads in Australia', *The Guardian* (online), 10 March 2020 <https://www.smh.com.au/politics/federal/facebook-imposes-new-transparency-rules-on-political-ads-in-australia-20200309-p54861.html>.

[135] Rob Leathern, 'Expanded Transparency and More Controls for Political Ads', *Facebook Newsroom* (Blog Post, 9 January 2020) <https://about.fb.com/news/2020/01/political-ads/>.

[136] Facebook, Submission No 140 to the Joint Select Committee on Electoral Matters, *Inquiry into and Report on All Aspects of the Conduct of the 2019 Federal Election and Matters Related Thereto* (8 October 2019) 3.

[137] @jack (Jack Dorsey) (Twitter, 31 October 2019, 7:05am) <https://twitter.com/jack/status/1189634360472829952>.

> *content that references a candidate, political party, elected or appointed government official, election, referendum, ballot measure, legislation, regulation, directive, or judicial outcome.*[138]

84. Prohibited advertisements are those which include references to 'political content', which encompass 'appeals for votes, solicitations of financial support, and advocacy for or against any of the above-listed types of political content'.[139] Advertisements of any type by candidates, political parties, or elected or appointed government officials are also prohibited.[140]

85. In addition, in April 2019, Twitter released its *Election Integrity Policy* which states that it prohibits 'attempts to use [its] services to manipulate or disrupt elections, including through the distribution of false or misleading information about the electoral process or when or how to vote'.[141] False and misleading information about how to participate in an election or other civic event or which intends to intimidate or dissuade voters from participating in an election is prohibited. Further, it is against the policy to create fake accounts which misrepresent their affiliation, or share content that falsely represents its affiliation, to a candidate, elected official, political party, electoral authority, or government entity.[142]

86. If a report is received, the outcomes depend on the severity and type of the violation as well as the accounts' history of previous violations. Consequences include tweet deletion, profile modifications (if the policy is breached within the profile information), or temporary or permanent account suspension.[143]

Potential options to counter foreign interference and disinformation

87. The Law Council's preliminary views are that any potential options to better protect Australians' right to privacy and strengthen Australia's resilience against foreign interference and disinformation through social media should be:

    (a) appropriately balanced against the right to freedom of expression and the constitutionally implied freedom of political communication;

    (b) proportionate and practicable; and

    (c) take the form of a multi-faceted approach, involving coordinated and collaborative action by the Australian Government, social media platforms and civil society.

A balancing of rights

88. The threats of foreign interference and disinformation are intertwined with human rights. As recognised by the European Commission:

---

[138] Twitter for Business, 'Political Content' (Web page) <https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html>.
[139] Ibid.
[140] Ibid.
[141] Twitter, 'Election Integrity Policy', *Help Center General Guidelines and Policies* (Web page, April 2019) <https://help.twitter.com/en/rules-and-policies/election-integrity-policy>.
[142] Ibid.
[143] Ibid.

> *Disinformation and foreign interference are a soft underbelly of our democracy, because they attack one of our dearest values – freedom of speech and the right to information.*[144]

89. Consideration of options to address disinformation and foreign interference will need to balance the right to freedom of expression, and the constitutionally implied freedom of political communication, with the protection of democratic rights and the right to privacy.[145] The balancing of interventions to target media literacy and disinformation with these rights has been acknowledged by the Australian Government.[146]

Right to privacy

90. The right to privacy is recognised as a fundamental human right in the *Universal Declaration of Human Rights* (**UDHR**), the *International Covenant on Civil and Political Rights* (**ICCPR**), the *Convention on the Rights of the Child* (**CRC**) and other instruments and treaties.[147]

91. Article 17 of the ICCPR states that:

> *(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *(2) Everyone has the right to the protection of the law against such interference or attacks.*[148]

92. Article 16 of the CRC uses similar terms in relation to children.[149]

93. Privacy is a fundamental human right that is essential in order to live with dignity and security. It is increasingly common for personal data to be collected with or without our knowledge through the internet, apps, and social media platforms which harness AI technology, as demonstrated by the Cambridge Analytica case. Data collection is often used to track, profile, and predict the behaviour of the population. Data collection is often a compulsory precondition to the provision of services, many of which in turn provide more data about an individual.[150]

94. The Law Council is concerned that laws protecting individuals against breach of privacy have not kept pace with technological developments, and there is a need for such protections to be reviewed and reformed. New technologies, such as those that enable corporations and governments to build up detailed profiles of individuals based on their

---

[144] Věra Jourová, 'Opening Speech' (Speech, Disinfo Horizon: Responding to Future Threats Conference, 30 January 2020) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_160>.
[145] Joint Standing Committee on Electoral Matters, *2019 Status Report,* 9 [3.14].
[146] Treasury, Australian Government, *Government Response to the Digital Platforms Inquiry*, 7.
[147] See *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd session, 183 plen mtg, UN Doc A/810 (10 December 1948) art 12; *International Covenant on Civil and Political Rights*, opened for signature 16 December 1976 (entered into force 23 March 1976) 999 UNTS 171 and 1057 UNTS 407 art 17; *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 16.
[148] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) art 17(1).
[149] *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 16.
[150] See Law Council of Australia, Submission to the Australian Human Rights Commission, *Human Rights and Technology* (25 October 2018) 17 [55] <https://www.lawcouncil.asn.au/docs/89d805e0-14d8-e811-93fc-005056be13b5/3533%20-%20Human%20Rights%20and%20Technology.pdf>.

personal data and browsing history, present an unprecedented scope for serious invasions of privacy.[151]

Democratic rights

95. Article 21 of the UDHR states:

> *(1) Everyone has the right to take part in the government of his country, directly or through freely chosen representatives.*
>
> *(2) Everyone has the right of equal access to public service in his country.*
>
> *(3) The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.*[152]

96. While the protection of free elections and electoral integrity is critical for democracy, efforts which involve the imposition of restrictions on content online may cause rise to concerns about the potential for regulation to result in disproportionate incursions on the right to freedom of expression.[153]

Right to freedom of speech

97. Under Article 19(1) of the ICCPR, everyone shall have the right to hold opinions without interference.[154] While freedom of opinion under Article 19(1) of the ICCPR is absolute, 'the absolute nature of the right ceases once one airs or otherwise manifests one's opinions'.[155]

98. The right to freedom of expression is contained in Article 19(2) of the ICCPR which provides that this right includes:

> *freedom to seek, receive and impart information and ideas of all kinds regardless of frontiers, either orally in writing or in print, in the form of art, or through any other media of his choice.*[156]

99. Article 19(3) of the ICCPR provides that the exercise of the rights provided for in Article 19(2) carries with it 'special duties and responsibilities'.[157] It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

    (a) for respect of the rights or reputations of others; and

---

[151] Ibid [56].
[152] *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd sess, 183 plen mtg, UN Doc A/810 (10 December 1948) art 21.
[153] Ethan Shattock, 'Fake News, Free Elections, and Free Expression: Balancing Fundamental Rights in Irish Policy Responses to Disinformation Online' (Paper, National University of Ireland Maynooth).
[154] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) art 19(1).
[155] Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (3rd ed, 2013) 591.
[156] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) art 19(2).
[157] Ibid art 19(3).

(b) for the protection of national security or of public order (*ordre public*), or of public health or morals.[158]

100. In its *General Comment 34: Article 19: Freedoms of Opinion and Expression* (***General Comment 34***), the United Nations Human Rights Committee (**UNHRC**) states in relation to freedom of expression that:

> *Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent they are compatible with paragraph 3.*[159]

Restriction for the protection of 'national security'

101. Paragraph 3 of Article 19 states that the right to freedom of expression can be limited for the protection of national security. Conformably with international human rights jurisprudence, the Law Council accepts that the protection of national security, inter alia, can justify restrictions on the right to freedom of expression as long as any such restrictions are provided by law and are necessary for the protection of national security.[160]

102. The UNHRC's *General Comment 34* provides that any restrictions must be 'necessary' for a legitimate purpose and must not be 'overbroad'. As to the latter, restrictive measures must:

(a) conform to the principle of proportionality;

(b) be appropriate to achieve their protective function;

(c) be the least intrusive instrument amongst those which might achieve their protective function; and

(d) be proportionate to the interest to be protected.[161]

103. The justifiable restriction on freedom of expression on the ground of national security is narrowly defined: this ground of restriction is invoked when the political independence or the territorial integrity of the state is at risk.[162]

---

[158] Ibid.
[159] Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Material and Commentary* (3rd ed, 2013) 599, citing Human Rights Committee, *General Comment 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [43].
[160] *International Covenant on Civil and Political Rights*, opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976) art 19(3).
[161] Human Rights Committee, *General Comment 34: Article 19: Freedoms of Opinion and Expression*, 102nd sess, Un Doc CCPR/C/GC/34 (12 September 2011) [33]-[34].
[162] Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Material and Commentary* (3rd ed, 2013) 612, citing United Nations Commission on Human Rights, *Siracusa Principles of the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, 41st sess, Agenda Item 18, UN Doc E/CN.4/1985/4 (28 September 1984) 6.

Freedom of Expression and 'Fake News', Disinformation and Propaganda

104. The United Nations, alongside other bodies, has considered this specific tension in the *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda* (**Joint Declaration**).[163] The Joint Declaration states:

> *States may only impose restrictions on the right to freedom of expression in accordance with the test for such restrictions under international law, namely that they be provided for by law, serve one of the legitimate interests recognised under international law, and be necessary and proportionate to protect that interest.*[164]

105. In that regard, 'general prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information"', are not necessary and proportionate.[165]

106. The Joint Declaration sets out: standards on disinformation and propaganda; the positive obligations on States to enable an environment for freedom of expression; the roles and responsibilities on 'intermediaries' (i.e. social media platforms) through facilitation of the enjoyment of the right to freedom of expression through digital technologies to respect human rights; and the regulatory measures that should be undertaken by journalists and media organisations.[166]

Freedom of political communication

107. In the context of the current Inquiry, the Law Council also highlights the effect of the constitutionally implied freedom of political communication, and notes that it is not amenable to alteration by legislation. The High Court of Australia has recognised the freedom of political communication as a fundamental common law right necessary for our system of representative government.[167]

108. The two-step test developed in *Lange v Australian Broadcasting Corporation* is as follows:

> *First, does the law effectively burden freedom of communication about government or political matters either in its terms, operation or effect? Second, if the law effectively burdens that freedom, is the law reasonably appropriate and adapted to serve a legitimate end the fulfilment of which is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government and the procedure prescribed by s 128 for submitting a proposed amendment of the Constitution to the informed decision of the people... If the first question is answered 'yes' and the second is answered 'no', the law is invalid.*[168]

---

[163] United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe, Representative on Freedom of the Media, the Organization of American States, Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights, Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda* (3 March 2017) <https://www.article19.org/resources/joint-declaration-on-freedom-of-expression-and-fake-news-disinformation-and-propaganda/>.

[164] Ibid art 1(a).

[165] Ibid 2(a).

[166] Ibid cls 1-4.

[167] *Australian Capital Television v Commonwealth* (1992) 177 CLR 106, 139 (Mason CJ). See also *Nationwide News v Wills* (1992) 177 CLR 1, 74 (Brennan J).

[168] *Lange v Australian Broadcasting Corporation* (1997) 145 ALR 96, 112.

109. While this implied freedom may be 'limited to what is necessary for the effective operation of that system of representative and responsible government provided for by the Constitution',[169] it nonetheless will have implications for attempts to address online political communication.

110. Regarding the limitations on this freedom, the following passage clarifies that the Australian Parliament may, in some circumstances, impose restrictions on the freedom of political communications, such as to balance the need of such measures with the importance of political discussion:

> *It is both simplistic and erroneous to regard any limitation on political advertising as offensive to the Constitution. If that were not so, there would be no blackout on advertising on polling day; indeed, even advertising in the polling booth would have to be allowed unless the demands of peace, order and decorum in the polling booth qualify the limitation. Though freedom of political communication is essential to the maintenance of a representative democracy, it is not so transcendent a value as to override all interests which the law would otherwise protect.*[170]

Proportionality and practicability

111. The Law Council supports measured regulation to increase the transparency of political advertising on Facebook, which is proportionate, reasonably appropriate and adapted to address the legitimate threat of disinformation and foreign interference.

112. Any regulation must place workable obligations on social media networks. This must be contrasted with previous attempts at regulation of social media, such as the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth), which the Law Council considered was not fit for purpose and had the potential to create an unintended chilling effect on industry in Australia.[171]

A multi-faceted approach

113. The nature of the problem of disinformation is complex and overlapping, involving issues pertaining to cybersecurity, national security, privacy, electoral integrity, media and advertising standards, transparency, and media literacy. Any effective response will need to account for these various aspects.[172]

114. In addition, the Australian Government has recognised that the approach requires collaborative and coordinated action between the Australian Government, industry and civil society.[173] The Australian Government has suggested that this includes:

---

[169] Ibid.
[170] *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106, 159 (Brennan J). See also Joint Select Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election*, 167 [7.35].
[171] Law Council of Australia, 'Livestream Laws Could Have Serious Unintended Consequences, Chilling Effect On Business' (Media Release, 4 April 2019) <https://www.lawcouncil.asn.au/media/media-releases/livestream-laws-could-have-serious-unintended-consequences-chilling-effect-on-business>.
[172] Luke Buckmaster and Tyson Wils, 'Responding to Fake News' (Parliamentary Library Briefing Book: Key Issues for the 46th Parliament, Parliament of Australia, July 2019) <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook46p/FakeNews>.
[173] Treasury, Australian Government, *Government Response to the Digital Platforms Inquiry*, 6.

> *the creation of a strong and sustainable news media ecosystem alongside educational initiatives for citizens to improve their ability to engage critically with online news and information sources.*[174]

115. As noted in the Introduction, this preliminary submission intends to canvass the key challenges to democracy posed by social media and how some international jurisdictions have sought to address such issues. Nonetheless, this submission now makes some preliminary suggestions on measures which the Law Council considers are worthy of consideration in the multifaceted approach which should be taken forward.

Increasing transparency in political advertising on Facebook

116. Requirements, legislative or otherwise, which would mandate social media platforms to establish public databases of political advertisements, which present data such as the amount spent on the advertisements, and by whom the money was spent, and targeting parameters, would be an important and significant step forward. This could be achieved in a number of ways. For example, as discussed above on page 23, Facebook extended its authorisation process and operation of the Ad Library to Australia without a legislated mandate.

117. Alternatively, the Australian Parliament could consider legislative measures to require platforms to do so. To this end, the Law Council would support the expansion of the reporting requirements placed on social media platforms for the purpose of the social media communication authorisation requirements in Part XXA of the Electoral Act. This may be achieved, for example, by legislatively mandating the collection and reporting of information relating to the posting of political advertising on social media platforms – similar to that required by the amendments to the *Canada Elections Act 2000* (see discussion below on page 36), which require platforms' compliance with the law to establish and maintain searchable databases of political advertisements, or as is proposed by the *Honest Ads Act 2019* in the US Senate (see discussion below on page 35).

Media literacy

118. As noted above on page 11, the research of the News and Media Centre in its *Digital News Report* has found that, while Australians are generally concerned about the dissemination of disinformation online, most Australian news consumers in the study indicated that they do not adopt any news verification behaviours.[175] Only 36 per cent reported that they compare the reporting of a story across news outlets to check its accuracy, and 26 per cent said they began to use more reliable news sources.[176] Critically, those who are concerned about disinformation online, or those who are interested in politics, are more likely to fact-check that than those who are not.[177]

119. The News and Media Centre's research found that 'there are significant stratifications in citizen's capacities to respond to false and/or manipulative information claims they encounter'.[178] It has recommended that the low rates of fact checking among Australian

[174] Ibid.
[175] News and Media Research Centre, Submission No 75 to the Joint Standing Committee on Electoral Matters, *Inquiry into and Report on All Aspects of the Conduct of the 2019 Federal Election and Matters Related Thereto* (2019) 6.
[176] Ibid.
[177] Ibid 7.
[178] Ibid 20.

news consumers points to the need for targeted programs to boost news and media literacy among voting age citizens.[179]

120. The Electoral Matters Committee has noted that:

> *increased social media literacy, as part of a strengthened civics and electoral education curriculum, is a vital component in facing the challenges posed by this new social media environment. Australians must be better equipped to critically discern and judge any media which seeks to influence their voting behaviour.*[180]

121. Specifically, it recommended that:

    (a) Australian Government consider ways in which media literacy can be enhanced through education programs that teach students not only how to create media, but also how to critically analyse it; and

    (b) AEC examine ways in which media literacy can be incorporated into a modern, relevant civics education program.[181]

122. Similarly, the *Digital Platforms Inquiry* echoed this sentiment, recommending measures to improve digital media literacy across the community 'to ensure all Australians are well equipped to identify and appropriately scrutinise low quality or unreliable news encountered through digital platforms'.[182]

123. Namely, the ACCC recommended that:

    (a) a Government program be established to fund and certify non-government organisations for the delivery of digital media literacy resources and training. It should be based on the frameworks currently used by the 'Online Safety Grants Program' and 'Be Connected' program, which are administered by the Office of the eSafety Commissioner;[183] and

    (b) there should be separate consideration of the approach to digital media literacy in schools as part of the broader review of the Australian Curriculum scheduled for 2020.[184]

124. The Law Council supports the recommendations of the ACCC and the Electoral Matters Committee, and is encouraged by the Australian Government's acknowledgment for the need of citizens to be equipped to engage critically with online news and information,[185] and its commitment to action in this regard. The Law Council welcomes the Australian Government's plan to explore models to establish a network of experts and organisations to develop media literacy materials and to include news and media literacy included within the scheduled review of the Australian curriculum.[186]

---

[179] Ibid.
[180] Joint Select Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election*, 60 [3.125].
[181] Ibid 182 [7.102]-[7.104].
[182] Australian Competition and Consumer Commission, *Final Report of the Digital Platforms Inquiry,* 368-9 [12.6.4].
[183] Ibid Recommendation 12.
[184] Ibid Recommendation 13; See Australian Government Department of Education and Training, 'Australian Curriculum' (Web page) <https://www.education.gov.au/australian-curriculum-0>.
[185] Ibid.
[186] Treasury, Australian Government, *Government Response to the Digital Platforms Inquiry*, 16.

Dedicated cyber manipulation body

125. The demonstrated effectiveness of the establishment of specialist bodies and taskforces dedicated to preventing and monitoring cyber manipulation of democratic processes can be seen in the discussion below from page 37 regarding the approaches adopted by other jurisdictions, such as in the US, the UK and the EU.

126. The Australian Government is continuing to obtain greater cooperation from platforms in terms of illegitimate advertising practices. However, for example, the AEC is not sufficiently resourced to actively and constantly monitor online interactions and generally relies on the reporting of offending unauthorised advertisements.[187]

127. The Law Council agrees with the recommendation of the Electoral Matters Committee that the Australian Government establish a permanent taskforce to prevent and combat cyber manipulation in Australia's democratic process and to provide transparent, post-election findings regarding any pertinent incidents.[188] This would bring greater transparency to platforms methods of regulation and moderation of the content on their platforms when it concerns disinformation.

Compliance with Australian laws

Facebook's compliance with domestic advertising laws

Unauthorised communications and paid advertisements on 'electoral matter'

128. During 2019, it was reported that Facebook had not adequately applied the authorisation rules set out by the Electoral Act (discussed above on page 15) to advertising on its platform and did not respond to AEC inquiries about the source of advertising in a timely manner.[189] Facebook's reported response was firstly that the advertising in question was not paid advertising and therefore was not required to comply with the authorisation requirements under Part XXA.[190] Four weeks after AEC first raised the issue with Facebook, it was agreed that the Page was paying for advertisements, however by this stage the group had already been removed by the administrator.[191]

129. The AEC considers that non-compliance with the authorisation rules are more serious cases of non-compliance, as this 'fails to provide the elector with the ability to discern the identity of the person responsible for the advertisement'.[192] Further, it considers that non-compliance which occurs during federal election periods to be serious cases of non-compliance as this has 'the potential to have a more significant and direct impact on the casting of votes'.[193]

---

[187] Christopher Knaus and Nick Evershed, 'Electoral Watchdog Powerless to Crack Down on Offshore Political Ads Targeting Australians', *The Guardian* (online, 24 July 2018) <https://www.theguardian.com/australia-news/2018/jul/24/australian-watchdog-unable-to-enforce-political-advertising-law-over-offshore-sites>.
[188] Joint Select Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election*, 181 [7.97].
[189] Pat McGrath, 'Facebook Probed by Australian Electoral Commission Over Mysterious Political Ads', *ABC News* (online, 26 February 2019) <https://www.abc.net.au/news/2019-02-26/facebook-electoral-commission-emails-reveal-political-ad-concern/10834736>.
[190] Ibid.
[191] Ibid.
[192] Australian Electoral Commission, 'Electoral Backgrounder: Electoral Communications and Authorisation Requirements' (Web page, 16 July 2019) <https://www.aec.gov.au/About_AEC/Publications/Backgrounders/authorisation.htm>.
[193] Ibid.

Overseas-hosted online electoral advertisements

130. It has been reported that challenges have arisen for the AEC when attempting to enforce the authorisation requirements when the unauthorised online advertising originates overseas.[194] Specifically, the difficulty arises when the author cannot be identified or refuses to comply with the AEC's requests.[195]

131. Paid advertisements which originate overseas can be required to have the authorisation particulars as mandated under Part XXA of the Electoral Act. For example, unauthorised paid advertisements which originate overseas can contravene section 321D when the conduct constituting the alleged contravention occurs wholly outside Australia but a result of the conduct occurs wholly or partly in Australia.[196]

132. It was reported that, during the same-sex marriage plebiscite campaigns, the AEC was asked to investigate a website, registered in Panama and hosted in the US, that was distributing homophobic material to support the no campaign.[197] Regarding this case, the AEC stated that it did not have available sufficient tools to enable remedial action and that, in this case, like many, the individual or group behind the advertisement was difficult to identify.[198]

International responses to cyber-enabled foreign interference and disinformation

133. The Law Council agrees with the Committee on Electoral Matters that the Australian Parliament must have regard to the work undertaken by committees of international parliaments which have sought to address the challenges to democracy caused by disinformation and digital technology.[199] Further, governments around the globe have developed a range of approaches, from educative to punitive, in attempts to counter these issues.[200] The Australian Government has recognised that Australia's approach to media literacy and disinformation should 'align with and support global initiatives'.[201]

134. The developments in the US, Canada, the UK, France and the EU are discussed below, as well as the International Grand Committee on Disinformation and 'Fake News' established in late 2018.

United States

135. The US Government and the Congress have undertaken numerous inquiries and produced many reports on foreign interference in its 2016 Presidential Election campaign. These include the US Senate Committee on Foreign Relations' report *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National*

[194] Christopher Knaus and Nick Evershed, 'Electoral Watchdog Powerless to Crack Down on Offshore Political Ads Targeting Australians', *The Guardian* (online, 24 July 2018) <https://www.theguardian.com/australia-news/2018/jul/24/australian-watchdog-unable-to-enforce-political-advertising-law-over-offshore-sites>.
[195] Ibid.
[196] *Commonwealth Electoral Act* (Cth) s 321E.
[197] Christopher Knaus and Nick Evershed, 'Electoral Watchdog Powerless to Crack Down on Offshore Political Ads Targeting Australians', *The Guardian* (online, 24 July 2018) <https://www.theguardian.com/australia-news/2018/jul/24/australian-watchdog-unable-to-enforce-political-advertising-law-over-offshore-sites>.
[198] Ibid.
[199] Joint Standing Committee on Electoral Matters, *2019 Status Report*, 16 [3.38].
[200] Ibid 9 [3.14].
[201] Treasury, Australian Government, *Government Response to the Digital Platforms Inquiry*, 7.

Security,[202] the US Senate Select Committee on Intelligence's report on *Russian Active Measures Campaigns and Interference in the 2016 US Elections*: *Russia's Use of Social Media*,[203] and the Office of the Director of National Intelligence's report on *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution*.[204]

136. Further, a grand jury in the District Court of Columbia returned an indictment presented by the Special Counsel's Office on thirteen Russian nationals and three Russian companies (including the Internet Research Agency) for committing federal crimes by interfering in the 2016 Presidential election.[205] The indictment classifies this offending as 'information warfare' with the objective 'to sow discord in the U.S. political system, including the 2016 U.S. presidential election' by actions such as:

    (a) posting derogatory information about a number of candidates, including supporting the Trump Campaign and disparaging Hillary Clinton. Defendants made various expenditures to carry out those activities, including buying political advertisements on social media in the names of US persons and entities;

    (b) staging political rallies in the US, while posing as US grassroots entities and US persons and without revealing their Russian identities and organisational affiliation; and

    (c) solicited and compensated real US persons to promote or disparage candidates.[206]

137. The indictment stated that, in order to carry out interference in US political and electoral processes without detection of their Russian affiliation, the defendants:

> *conspired to obstruct the lawful functions of the US government through fraud and deceit, including by making expenditures in connection with the 2016 US presidential election without proper regulatory disclosure; failing to register as foreign agents carrying out political activities within the United States; and obtaining visas through false and fraudulent statements.*[207]

138. Additionally, a Congressional Bill, the *Honest Ads Act 2019*,[208] is currently in the US Senate. A version of this Bill was first introduced in 2017.[209] The *Honest Ads Act 2019* proposes to address apparent loopholes in US campaign funding laws by subjecting internet advertisements to the same rules as TV and radio advertisements.[210] Under current US law, foreign nationals are banned from paying for TV and radio advertisements that mention political candidates, but this does not extend to online ads.[211] The proposed legislation would also require technology companies to 'make

[202] US Senate Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security* (Report, January 2018) <https://www.foreign.senate.gov/imo/media/doc/SPrt_115-21.pdf>.
[203] US Senate Select Committee on Intelligence, *Russia's Use of Social Media*.
[204] Office of the Director of National Intelligence's, *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution* (Report, 6 January 2017) <https://www.dni.gov/files/documents/ICA_2017_01.pdf>.
[205] *United States of America v Internet Research Agency LLC* (Indictment of the United States District Court of Colombia, 16 February 2018) <https://www.justice.gov/opa/press-release/file/1035562/download>.
[206] Ibid 4 [6].
[207] Ibid [7].
[208] *Honest Ads Act*, S 1356, 116th Congress (2019) <https://www.congress.gov/bill/116th-congress/senate-bill/1356/text>.
[209] *Honest Ads Act*, S 1989, 115th Congress (2017).
[210] *Honest Ads Act*, S 1356, 116th Congress (2019) cl 5.
[211] *Federal Election Campaign Act of 1971*, 52 USC § 30101(22).

reasonable efforts' to prevent foreign nationals from buying political ads on their platforms.[212]

139. Further, the *Honest Ads Act 2019* seeks to strengthen transparency about who is funding online advertisements. Currently, anyone who pays for a political advertisement on TV must include in the advertisement a disclaimer identifying themselves and the broadcaster must keep public records of political advertisement purchases.[213] However, this does not extend to online advertisements. The *Honest Ads Act 2019* seeks to extend the disclaimer requirements for TV and radio political advertisements to online advertisements.[214]

140. The *Honest Ads Act* would also require social media platforms to maintain public databases of all online political advertisements, regardless of whether they mention specific candidates and make publicly available information such as target audience, timing, and payment information.[215] As noted above on page 22, Facebook's Ad Library operates in the US without a legislative mandate to do so. Facebook has noted its support for the *Honest Ads Act* as a measured way to prevent election interference.[216]

141. Lastly, leading up to the 2020 Presidential election, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (**CISA**), the US' lead federal agency responsible for national election integrity, has launched #Protect2020.[217]

142. Through #Protect2020, CISA operates various outreach programs with election officials to identify and plan for potential vulnerabilities to election infrastructure for the 2020 election season. Additionally, it engages with political campaigns, political parties, and political committees at the national level in preparation for the 2020 elections.[218]

143. There is also a webpage designed to be a starting point for resources on election security for the public as well as officials.[219] Within the #Protect2020 project sits a Countering Foreign Interference Task Force, which is tasked with building resilience to foreign interferences, particularly information activities such as disinformation and misinformation.[220] As it considers that foreign interference 'requires a whole of society approach', it publishes publicly available, digestible and non-complex tools which explain topics including foreign interference and social media bots,[221] and provides the public with fact sheets on how to better recognise foreign interference and disinformation.[222]

---

[212] *Honest Ads Act*, S 1356, 116th Congress (2019) cl 9.
[213] *Federal Election Campaign Act of 1971*, 52 USC § 30104(f)-(j).
[214] *Honest Ads Act*, S 1356, 116th Congress (2019) cl 7.
[215] Ibid cl 8.
[216] Mark Zuckerberg, 'Big Tech Needs More Regulation' *Financial Times* (18 February 2020).
[217] Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, '#PROTECT2020' (Web page) <https://www.cisa.gov/protect2020>.
[218] Ibid.
[219] Ibid.
[220] Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, 'Foreign Interference' (Web page) <https://www.cisa.gov/publication/foreign-interference>.
[221] Department of Homeland Security, Department of Homeland Security 'Foreign Interference Taxonomy' (Fact Sheet, July 2018) <https://www.cisa.gov/sites/default/files/publications/19_0717_cisa_foreign-influence-taxonomy.pdf>; Cybersecurity and Infrastructure Security Agency, Department of Homeland Security 'The War on Pineapple: Understanding Foreign Interference in 5 Steps' (Fact Sheet, July 2019) <https://www.cisa.gov/sites/default/files/publications/19_1008_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf>; National Protection and Programs Directorate, Department of Homeland Security, 'Social Media Bots Overview' (Fact Sheet, May 2018) <https://www.cisa.gov/sites/default/files/publications/19_0717_cisa_social-media-bots-overview.pdf>.
[222] Department of Homeland Security, Department of Homeland Security, 'Disinformation Stops With You' (Fact Sheet) <https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_nrmc-Disinformation-Stops-With-You_0.pdf>.

Canada

144. The Canadian House of Commons Standing Committee on Access to Information, Privacy and Ethics (**Canadian House of Commons Committee**) released its report *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly* in December 2018.[223] In broad terms, its recommendations related to:

    (a) removing the exemption for political parties and political third parties from Canadian data privacy law;

    (b) strengthening the measures which seek to prevent foreign funding and influence in domestic elections, including foreign charitable funding;

    (c) strengthening transparency of political advertising by amending Canadian electoral law to require:

        (i) identity authentication when placing political advertisements online;

        (ii) social media platforms to create searchable and machine-readable databases of online advertising that are user-friendly and allow anyone to find advertisements using filters, such as the person or organisation who funded the ad, the political issue covered, the period during which the advertisement was online and the demographics of the target audience;

    (d) increasing social media platforms' responsibility for online content through legislation to require:

        (i) labelling of content produced automatically or logarithmically;

        (ii) identification and removal of inauthentic and fraudulent accounts impersonating others for malicious reasons;

        (iii) adherence to a code of practice which would prohibit deceptive or unfair practice and require prompt responses to hate speech and harassment and removal of defamatory, fraudulent and maliciously manipulated content;

        (iv) clearly label political advertising;

    (e) undertake further research on:

        (i) potential economic harms caused through data-opolies;

        (ii) how cyber threats affect democratic institutions and electoral systems;

        (iii) the impacts of online disinformation and misinformation; and

    (f) invest in digital literacy initiatives.224

145. In December 2018, the *Election Modernization Act 2018* was passed by the Canadian Parliament.[225] This amended the *Canada Elections Act 2000* to require digital platforms

[223] Canadian House of Commons Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly* (Report, December 2018) <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf>.
[224] Ibid.
[225] *Election Modernization Act*, SC 2018, c 31.

to increase transparency with respect to advertising online.[226] Major online platforms must maintain a registry of partisan and election advertising published during the pre-election and election periods.[227] The registry must include a copy of the advertising message, and the name of the person who authorised it and the financial agent of the advertisement.[228] This complements the requirement for political parties and third parties[229] to identify themselves on their partisan and election advertising during these periods.[230] The *Election Modernization Act 2018* also prohibits foreign entities from spending any money to influence federal elections and third-party organisations are prohibited from using foreign funds for their partisan activities and advertising, irrespective of when it is taking place.[231] The Canadian Government considers that this measure 'represents an important step towards ensuring that Canadians have the tools to know who is trying to influence their vote'.[232]

146. In January 2019, the Canadian Government released its plan to safeguard Canada's 2019 federal election.[233] This plan involves four pillars: enhancing citizen preparedness; improving organisational readiness; combatting foreign interference; and expecting social media platforms to act.[234] On the latter point, leading up to the Canadian federal election, in May 2019 a declaration to guide social and digital platforms to ensure integrity was released. The *Canada Declaration on Electoral Integrity Online* establishes a common understanding with the platforms about their responsibilities in the online democratic space.[235]

United Kingdom

147. The UK Government has undertaken numerous inquiries into the impacts of social media. These have led to legislative and non-legislative reforms in attempt to address the challenges posed by social media to democratic processes, including the establishment of committees and programmes, development of codes of conduct and practice, and law reform proposals, addressing areas including the use of data in politics and political digital advertising. Some of these are discussed below.

Data analytics for political micro-targeting purposes

148. In May 2017, the UK Information Commissioner's Office (**ICO**) announced that its formal investigation into the use of data analytics for political purposes after allegations were made about the 'invisible processing' of people's personal data and the micro-targeting of political adverts during the EU Referendum.[236]

---

[226] *Canada Elections Act,* SC 2000, c 9, pt 16, as amended by *Election Modernization Act 2018*, SC 2018, c 31, s 325.1-325.2.
[227] Ibid ss 325.1(1), (4).
[228] Ibid s 325.1(3).
[229] Ibid s 349, definition of 'third party'.
[230] Ibid pt 17, as amended by *Election Modernization Act 2018*, SC 2018, c 31.
[231] Ibid ss 349(4), 351.1, as amended by *Election Modernization Act 2018*, SC 2018, c 31.
[232] Government of Canada, 'Expecting Social Media Platforms To Act' (Web page, 9 July 2019) <https://www.canada.ca/en/democratic-institutions/news/2019/01/encouraging-social-media-platforms-to-act.html>.
[233] Government of Canada, 'Government of Canada Unveils Plan to Safeguard Canada's 2019 Election' (Media Release, 30 January 2019) <https://www.canada.ca/en/democratic-institutions/news/2019/01/government-of-canada-unveils-plan-to-safeguard-canadas-election.html>.
[234] Ibid.
[235] Government of Canada, 'Canada Declaration on Electoral Integrity Online' (Web page, 27 May 2019) <https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/declaration-electoral-integrity.html>.
[236] Robert Booth, 'Inquiry Launched Into Targeting Of UK Voters Through Social Media', *The Guardian* (online, 18 May 2017) <https://www.theguardian.com/technology/2017/may/17/inquiry-launched-into-how-uk-parties-target-voters-through-social-media>.

149. In July 2018, the UK ICO published the report, *Democracy Disrupted? Personal Information and Political Influence,* which covered the policy recommendations from the investigation.[237] In November 2018, the UK ICO released its report, *Investigation into the Use of Data Analytics in Political Campaigns*, which provides a summary of the investigation undertaken.[238] The following details were revealed in the latter report about how the misuse of personal data on Facebook occurred:

    (a) In summary, there was an app, referred to as *This Is Your Digital Life*, whereby Facebook users undertook a 'My Personality' quiz. This app was accessed by up to approximately 320,000 Facebook users by taking a detailed personality test while logged into their Facebook account. In addition to the data collected directly from the personality test itself, the app utilised the Facebook login in order to request permission from the app user to access certain data from their Facebook accounts. The app also requested permission from users of the app to access the following categories of data about their Facebook Friends. At the time, this was permitted by Facebook's first version of its Graph Application Platform Interface (API V1), which permitted third party app developers access to a wealth of data concerning Facebook users and their Facebook friends.

    (b) The app then took a Facebook user's answers to the app survey and used them to make predictions about the Facebook user. This information was then combined with other information taken from the user's Facebook profile, such as the Pages the Facebook user had liked and used to build a data model about that individual which could predict how the user was likely to vote. However, because of the configuration of API V1, the app also received the public profile information about the app users' Facebook friends, including their Facebook likes. As such, *This Is Your Digital Life* was able to provide modelled data about the 'app' user and their Facebook friends whose privacy settings allowed access by third party apps.

    (c) Some of this data was subsequently used by Cambridge Analytica.[239] Cambridge Analytica's internal data scientists performed data modelling and created 'proprietary data models' that they then used during their political targeting work in the US and UK.[240]

150. The UK ICO's investigation concluded that while Facebook produced a range of policies for developers who deployed apps on their platform, Facebook did not take sufficient steps to prevent apps from collecting data in contravention of data protection law.[241] The UK ICO issued Facebook with the maximum monetary penalty of £500,000 available under the previous data protection law for lack of transparency and security issues relating to the harvesting of data.[242] It found that Facebook contravened the first and seventh data protection principles under the *Data Protection Act 1998* (UK).[243]

---

[237] Cabinet Office, United Kingdom, *Protecting the Debate: Intimidation, Influence and Information* (Report, July 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730209/CSPL.pdf>.
[238] Information Commissioner's Office, *Investigation into the Use of Data Analytics in Political Campaigns* (Report, 6 November 2018) <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>.
[239] Ibid 27.
[240] Ibid.
[241] Ibid.
[242] Ibid 38 [3.2.4].
[243] The first principle is the obligation to handle and deal with data fairly and lawfully. The seventh principle is the obligation that data is protected by appropriate security: The Department of Human Resources and

151. In addition, the UK ICO released in August 2019 draft guidance on political campaigning.[244] This guidance is tailored specifically to political campaigners on how to comply with the *General Data Protection Regulation* and the *Data Protection Act 2018* (UK).[245]

Disinformation and 'fake news'

152. The UK Government has also set up a parliamentary committee dedicated to the issue of disinformation and digital disruption. In April 2019, the Sub-Committee on Disinformation was established to be 'Parliament's institutional home for matters concerning disinformation and data privacy and their impact on democracy'.[246] The Sub-Committee on Disinformation was set up to continue the work commenced by the UK House of Commons Committee on disinformation and 'fake news'.

153. In January 2017, the UK House of Commons Committee launched an inquiry into disinformation and fake news.[247] In November 2018, representatives from eight countries joined the UK House of Commons Committee for a meeting, known as an 'International Grand Committee',[248] at which they signed the *International Principles on the Regulation of Tech Companies*.[249] After the final report of the UK House of Commons Committee was released in February 2019,[250] the International Grand Committee met a further three times during 2019 and agreed to a set of principles 'to advance international collaboration in the regulation of social media to combat harmful content, hate speech and electoral interference online'.[251]

154. The final report of the UK House of Commons Committee considered the data analytics issues involving Cambridge Analytica and Facebook, as well as advertising and political campaigns, foreign influence in political campaigns and digital literacy. It provided 48 recommendations on issues, ranging from reform to competition and consumer law and privacy law, to regulatory approaches to reduce online harms on social media, the use

---

Change Information Rights and Information Security Service, *Data Protection Act 1998: Personal Information About Constituents and Others* (Paper of Advice for Members and their Staff, March 2015) <https://www.parliament.uk/documents/foi/Advice-for-Members-and-Data-Protection-Feb15-WEB.pdf>

[244] United Kingdom Information Commissioner's Office, *Draft Framework Code for the use of Personal Data in Political Campaigning* (Draft Framework Code for Consultation, 8 August 2019) <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>.

[245] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC* (General Data Protection Regulation) [2016] OJ L 119/1.

[246] House of Commons Digital, Culture, Media and Sport Committee, *The Launch of the Sub-Committee on Disinformation* (Tenth Report of Session 2017–19, 2 April 2019) <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/2090/2090.pdf>.

[247] Parliament of the United Kingdom, ''Fake News' Inquiry Launched, *Commons Select Committee* (Web page, 30 January 2017) <https://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/news-parliament-2015/fake-news-launch-16-17/>.

[248] Centre for International Governance Innovation, 'Timeline: The International Grand Committee on Disinformation and "Fake News"', *Democracy, Emerging Technology, Internet Governance* (Web page, 20 January 2019) <https://www.cigionline.org/subject/democracy>.

[249] House of Commons Digital, Culture, Media and Sport Committee, *Final Report on Disinformation and 'Fake News',* 7 [1], 99 annex 2.

[250] Ibid 70 [242].

[251] Centre for International Governance Innovation, 'Timeline: The International Grand Committee on Disinformation and "Fake News"', *Democracy, Emerging Technology, Internet Governance* (Web page, 20 January 2019) <https://www.cigionline.org/subject/democracy>. Parliamentarians from Australia, Finland, Estonia, Georgia, Singapore, UK and the US travelled to Dublin attended the meeting: Department of the House of Representatives, 'International Grand Committee Meets in Dublin and Agrees Principles to Advance Global Regulation of Social Media' (Media Release, 17 November 2019) <https://www.aph.gov.au/About_Parliament/House_of_Representatives/About_the_House_News/Media_Releases/International_Grand_Committee_meets_in_Dublin>.

of personal data by political parties for political campaigning,[252] and strengthening accountability and oversight of strategic communications companies.[253]

155. Of most relevance to this inquiry are the UK House of Commons Committee's recommendations relating to political advertising, foreign interference and funding in election processes and media literacy. It was recommended that:

    (a) electoral law be updated to cover 'modern' campaigning, including:

        (i) the way in which the law defines digital campaigning, including definitions of what constitutes online political advertising, such as agreed types of words that continually arise in advertisements that are not sponsored by a specific political party;[254]

        (ii) acknowledging the role and power of unpaid campaigns and Facebook Groups that influence elections and referendums (both inside and outside the designated period);[255]

        (iii) increased transparency of online political campaigning, including micro-targeted campaigns, by placing clear, persistent banners on all paid-for political adverts and videos, indicating the source, the advertiser and country of origin;[256]

        (iv) introduction of a category for digital spending on campaigns and explicit rules surrounding designated campaigners' roles and responsibilities;[257]

        (v) updating and expanding the powers of the Electoral Commission to compel social media companies to provide information relevant to their inquiries;[258]

        (vi) creation of an independent, publicly accessible and searchable repository of political advertising items which provides the details of who is paying for the advertisements, which organisations are sponsoring the advertisement and who is being targeted by the advertisements;[259]

        (vii) address the issue of shell companies and other professional attempts to hide identity in advertisement purchasing, especially around political advertising;[260]

    (b) transparency laws around political donations be strengthened and expanded;[261]

    (c) foreign interference in elections be addressed, including further inquiries be undertaken to examine whether current legislation is sufficient to protect the

[252] House of Commons Digital, Culture, Media and Sport Committee, *Final Report on Disinformation and 'Fake News',* Recommendations 3-6 (regulation and online harms), Recommendations 7-9 (privacy law), Recommendations 26-27 (personal information in political campaigning).
[253] Ibid Recommendations 41-43.
[254] Ibid Recommendation 20.
[255] Ibid.
[256] Ibid Recommendation 21, 23.
[257] Ibid Recommendation 23.
[258] Ibid Recommendation 24.
[259] Ibid Recommendation 25.
[260] Ibid Recommendation 29.
[261] Ibid Recommendation 32.

electoral process from foreign influence, particularly foreign funding of campaigns and political donations;[262]

(d) a foreign agencies registration scheme be introduced to require political actors to make public disclosure of relationships with foreign principles;

(e) social media companies be required to publicise any instances of disinformation and share information they have about foreign interference on their sites including who has paid for political advertisements, who has seen the advertisements, and who has clicked on the advertisements;[263]

(f) digital literacy be the fourth pillar of education, along with reading, writing and maths and a comprehensive cross-regulator strategy developed to promote digital literacy.[264]

156. Further, an independent review was undertaken by Dame Frances Cairncross which examined the sustainability of high-quality journalism in the UK.[265] Specifically, it investigated:

> *the current and future market environment facing the press and high-quality journalism in the UK, including the role played by content and data flows and digital advertising, and the impact of search, social media and news aggregation platforms. It considered the different ways the press is adapting to the digital environment, including the emergence of new business models. It also looked into the impact technological developments are having on consumers, and whether digital advertising is encouraging 'clickbait' or the spread of disinformation.*[266]

157. This report, *The Cairncross Review: A Sustainable Future for Journalism* (**Cairncross Review Report**), was also released in February 2019.[267] This review considered different options for addressing concerns about what, and how, news is presented online, and consumers' capacity to assess the quality of online news.[268] The Cairncross Review Report notes that it had considered whether online platforms should be encouraged not only to downgrade or remove disinformation, but also to prioritise or give prominence to high-quality news.[269] On this point, the Cairncross Review Report concluded against this approach, noting:

> *to make this a binding constraint on the platforms would be difficult, given how hard it is to define high-quality news, and the extent to which the content that users see is a reflection of the choices they make themselves.*[270]

---

[262] Ibid Recommendation 34, 36.
[263] Ibid Recommendation 38.
[264] Ibid Recommendation 46-48.
[265] Dame Frances Cairncross, *The Cairncross Review: A Sustainable Future For Journalism* (Final Report, 12 February 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf>.
[266] Department for Digital, Culture, Media and Sport, *Government Response to the Cairncross Review: A Sustainable Future for Journalism* (Policy Paper, 27 January 2020) <https://www.gov.uk/government/publications/the-cairncross-review-a-sustainable-future-for-journalism/government-response-to-the-cairncross-review-a-sustainable-future-for-journalism>.
[267] Dame Frances Cairncross, *The Cairncross Review: A Sustainable Future For Journalism* (Final Report, 12 February 2019).
[268] Ibid 94.
[269] Ibid.
[270] Ibid.

158. Additionally, the Cairncross Review Report noted that it examined whether online platforms should be required to accept the same legal responsibilities as news publishers, including legal liability for publishing false stories.[271] The Cairncross Review Report also concluded against this approach, noting:

> *this proposal does not recognise the fundamental difference between distributors of news content, such as the platforms, and creators of content. If platforms were liable for all content on their services, they would be forced to vet everything they, or users, uploaded, placing strict constraints on what could be shared or surfaced. The overall effect might well be to reduce the online availability of news, and to harm users (who clearly value the online platforms' aggregation services). In other words, this proposal goes too far.*[272]

159. Instead, the Cairncross Review Report recommended that while platforms have developed initiatives to help users identify the reliability and trustworthiness of sources, these efforts must expand with appropriate oversight by government regulator.[273] It was recommended that, initially, the only requirement would be for platforms to report on their measures so that the regulator could gather information. In the longer term, it would be envisaged that the regulator would work with platforms and businesses to develop a 'best practices guide' for presentation of news on platforms.[274] The Cairncross Review Report also recommended that the UK Government work with all relevant stakeholders to develop a media literacy strategy, as it is critical to the functioning of democracy that all individuals are armed with critical literacy skills to navigate and evaluate the volume of online information and distinguish disinformation from accurate reports.[275]

160. The UK Government's response to both the UK House of Commons Committee's report, published in May 2019,[276] and the Cairncross Review Report, published in January 2020,[277] frequently referred to its *Online Harms White Paper* which was published in April 2019.[278]

161. The *Online Harms White Paper* commits to introducing an independent regulator which will enforce Codes of Practice and a Statutory Duty of Care.[279] The new regulator's *Code of Practice for Disinformation* is intended to include guidance for organisations on improving the transparency of political advertising, helping to meet any requirements in electoral law.[280] It is expected to also include a number of steps for the new regulator to include in a *Code of Practice for Disinformation*, proposing that responsibilities could be placed on companies to implement measures to increase transparency of political advertising and ensure that their users 'can clearly distinguish advertisements from

---

[271] Ibid.
[272] Ibid.
[273] Ibid 95.
[274] Ibid.
[275] Ibid.
[276] House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Final Report: Government Response to the Committee's Eighth Report of Session 2017* (Seventh Special Report of Session 2017–19, 9 May 2019) <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/2184/2184.pdf> ('*Government Response to the Final Report on Disinformation and 'Fake News"*).
[277] Department for Digital, Culture, Media and Sport, *Government Response to the Cairncross Review: A Sustainable Future for Journalism* (Policy Paper, 27 January 2020).
[278] Secretary of State for Digital, Culture, Media and Sport and the Secretary of State for the Home Department, *Online Harms White Paper* (April 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf>.
[279] Ibid 194-5.
[280] House of Commons Digital, Culture, Media and Sport Committee, *Government Response to the Final Report on Disinformation and 'Fake News'*, 11.

organic content'.[281] While the *Code of Practice for Disinformation* is to be ultimately determined by the independent regulator, the UK Government recommended that it should include the requirement for having clear reporting options for users to flag content and accounts they believe to be false or misleading.[282] At the time of writing, the UK Government is yet to establish the new regulator or release the proposed *Code of Practice on Disinformation*.[283]

162. The importance of this issue in the UK Government's agenda was highlighted in the Queen's Speech delivered on 19 December 2019, which noted that the UK Government intends to 'develop legislation to improve internet safety for all' in a manner which promotes freedom of speech.[284]

Strengthening electoral integrity

163. In July 2019, the UK Cabinet Office launched the 'Defending Democracy Programme' which has been established to:

    (a) protect and secure UK democratic processes, systems and institutions from interference, including from cyber, personnel and physical threats;

    (b) strengthen the integrity of UK elections;

    (c) encourage respect for open, fair and safe democratic participation; and

    (d) promote fact-based and open discourse, including online.[285]

164. As part of this program, the UK Government plans to undertake a consultation on electoral integrity.[286]

Political digital advertising

165. The report, *Democracy Disrupted? Personal Information and Political Influence,* considered issues such as voter intimidation and foreign influence in elections, in addition to digital political advertising.[287] Specifically, it sought comments on whether the UK Government should extend electoral law requirements for an imprint on campaigning materials to electronic communications.[288]

---

[281] Ibid 9.
[282] Ibid 23
[283] In February 2020 the UK Government released a paper, *Online Harms White Paper - Initial Consultation Response*, which sets out the feedback it received, its preliminary views and that it is in the process of implementing legislative and non-legislative measures to implement the proposals in the White Paper: Secretary of State for Digital, Culture, Media and Sport and the Secretary of State for the Home Department, *Online Harms White Paper - Initial Consultation Response* (Report, 12 February 2020) <https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response>.
[284] Queen of the United Kingdom, 'Queens Speech' (10 December 2019) <https://www.gov.uk/government/speeches/queens-speech-december-2019>.
[285] United Kingdom, *Parliamentary Debates,* House of Commons, 22 July 2019, vol 663, col 73WS (Mr David Lidington) <https://hansard.parliament.uk/commons/2019-07-22/debates/19072238000019/DefendingDemocracyProgramme>.
[286] United Kingdom, *Parliamentary Debates,* House of Commons, 5 November 2019, col HCWS100 (Oliver Dowden) <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2019-11-05/HCWS100/>.
[287] Cabinet Office, United Kingdom, *Protecting the Debate: Intimidation, Influence and Information* (Report, July 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730209/CSPL.pdf>.
[288] Ibid 44-50.

166. Under current electoral law, candidates, political parties and non-party campaigners are currently required to have an imprint on any printed election material, to demonstrate that they have produced it.[289] However, this requirement does not currently extend to online material.[290] The UK Government considers that 'extending this to include digital communications is essential for promoting fact-based political debate and tackling disinformation online'[291] and in May 2019 committed to introducing a digital imprints regime.[292]

167. As at 9 February 2020, there have not been any reforms in this regard but the UK Government has stated that it maintains its commitment 'to extending regulations covering the identification of campaigners offline to the online sphere and commits to launching 'a consultation on electoral integrity that will consider measures to …refresh our laws for the digital age'.[293]

168. In addition, the UK Government worked with the Electoral Commission in 2019 to publish statutory Codes of Practice for registered parties and candidates on electoral expenses which provides clarity on digital campaigning election expenses.[294]

Digital advertising

169. Furthermore, the Centre for Data Ethics and Innovation, an independent advisory body set up by the UK Government on the ethical use of AI and data-driven technology, undertook two projects looking at microtargeting and algorithmic bias to inform the UK Government's approach to ensuring these practices are used legitimately online.[295] The report on the former was released in February 2020, which, in general terms, recommended the following:

    (a) new systemic regulation of the online targeting systems that promote and recommend content like posts, videos and adverts;

    (b) powers to require platforms to allow independent researchers secure access to their data to build an evidence base on issues of public concern - from the potential links between social media use and declining mental health, to its role in incentivising the spread of misinformation;

---

[289] Cabinet Office, United Kingdom, *Protecting the Debate: Intimidation, Influence and Information: Government Response* (May 2019) 33 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/799873/Protecting-the-Debate-Government-Response-2019.05.01.pdf>.
[290] Lorraine Conway, *Political Advertising* (House of Commons Library, Briefing Paper No 8673, 1 November 2019) <http://researchbriefings.files.parliament.uk/documents/CBP-8673/CBP-8673.pdf>.
[291] House of Commons Digital, Culture, Media and Sport Committee, *Government Response to the Final Report on Disinformation and 'Fake News'*, 9-10.
[292] Sally Dray, *Online Political Advertising: On a Road to Regulation?* (House of Lords, Library Briefing, 5 February 2020) 1.
[293] Ibid.
[294] The Electoral Commission (UK), 'Response to Feedback on the Codes of Practice on Spending by Candidates and Political Parties Consultation' (Web page) <https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-views-and-research/our-consultations/response-feedback-codes-practice-spending-candidates-and-political-parties-consultation>. See, eg, The Electoral Commission (UK), *Code of Practice for Candidates* <https://www.electoralcommission.org.uk/sites/default/files/2019-08/Draft%20codes%20of%20practice%20for%20candidates%20%28PDF%29.pdf>.
[295] Centre for Data Ethics and Innovation, *Review of Online Targeting: Final Report and Recommendations* (Final Report, February 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/864167/CDEJ7836-Review-of-Online-Targeting-05022020.pdf>.

(c) platforms to host publicly accessible online archives for 'high-risk' adverts, including politics, 'opportunities' (e.g. jobs, housing, credit) and age-restricted products; and

(d) steps to encourage long-term wholesale reform of online targeting to give individuals greater control over how their online experiences are personalised.[296]

170. Furthermore, a report prepared by the Digital Competition Expert Panel was published in March 2019 on online advertising in the UK. [297] This assessed the wider impact online advertising has on the economy and society and presented 'recommendations on changes to competition and pro-competition policy to help unlock the opportunities of the digital economy'.[298]

France

171. In November 2018, France passed *The Law Against the Manipulation of Information*.[299] This legislation seeks to:

> *target the widespread and extremely rapid dissemination of fake news by means of digital tools, in particular through the dissemination channels offered by social networks and media outlets influenced by foreign states.*[300]

172. The French Government has explained that the measures in this legislation are aimed at targeting attempts to influence election results such as those which were seen during the US 2016 Presidential Election and the EU membership referendum in the UK.[301]

173. French law requires that during campaign periods (three months prior to the election date), digital platforms must provide users with 'information that is fair, clear and transparent' on how their personal data is being used and platforms must disclose any money they have been given to promote certain information.[302]

174. Further, *The Law Against the Manipulation of Information* introduced an injunction power for judges to remove online articles which are determined to constitute disinformation.[303] The legislation defines disinformation as 'inexact allegations or imputations, or news that falsely report facts, with the aim of compromising the outcome of an election'.[304] An application for an injunction must be filed by a political group, public authority or individual that alleges that there has been 'deliberate, either artificial or automatic, and massive' dissemination of fake and misleading information on an online communication service.[305] In this instance, the judge may act proportionally with any means to halt the

[296] Centre for Data Ethics and Innovation, 'CDEI Calls for Overhaul of Social Media Regulation' (Press Release, 4 February 2020) <https://www.gov.uk/government/news/cdei-calls-for-overhaul-of-social-media-regulation>.
[297] Digital Competition Expert Panel, *Unlocking Digital Competition* (Report, March 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf>.
[298] Ibid 2-3.
[299] *Loi n° 2018-1202 du 22 Decembre 2018* (France) JO, 22 Decembre 2018.
[300] French Government, 'Against Information Manipulation' (Web page) <https://www.gouvernement.fr/en/against-information-manipulation>.
[301] Ibid.
[302] Ibid; Australian Competition and Consumer Commission, *Final Report of the Digital Platforms Inquiry,* 366.
[303] *Le Code Électoral* (France) art 163-2.
[304] Ibid.
[305] Ibid. See also Library of the Congress, *Initiatives to Counter Fake News: France* (Law Library, Legal Report, 6 November 2019) <https://www.loc.gov/law/help/fake-news/france.php#III>.

dissemination and must do so with 48 hours of receiving the notification of the allegation.[306]

175. Another important part of this legislation is that it establishes a 'duty for online platforms to cooperate in fighting against the dissemination of false information'.[307] Online platforms are required to establish a tool for users to report disinformation, including when it is content promoted on behalf of a third party.[308] Platforms are also required to implement additional measures, in particularly in relation to:

    (a) transparency about how their algorithms function;

    (b) promoting content from mainstream press agencies;

    (c) taking action against accounts that 'propagate massive misinformation';

    (d) disclosing key information relative to sponsored content and the 'identity of individuals or organizations that promoted them'; and

    (e) media literacy initiatives.[309]

176. This legislation also gives the French national broadcasting agency the power to prevent, suspend and stop the broadcasts of television services that are controlled by foreign states or are influenced by these states, and which are detrimental to the country's fundamental interests.[310] The legislation contains penalties for violation of these provisions, including one year in prison and a fine of €75,000.[311] Further, the French national broadcasting agency monitors platforms' compliance with the law and publishes regular reports on the effectiveness of measures enacted by platforms.[312]

177. Twitter's General Guidelines and Policies note that it is required by French law to provide a means for users to report false information that could alter a vote's sincerity or disturb the public order. Twitter does not take action on these reports on an individual basis but uses the 'reports to inform how [it] defends [the] platform against manipulation'.[313]

European Union

178. The European Commission (**Commission**) has been extremely active in taking a softer regulatory approach to disinformation, commencing in 2015, and implementing a broad range of measures such as specialist policy and regulatory bodies, codes of practice and risk management and alert systems. Some of these are discussed in turn.

---

[306] Ibid.
[307] *Loi n° 190 du 20 Novembre 2018* (France) JO, 28 November 2018, art 11.
[308] Ibid.
[309] *Le Code Électoral* (France) art 112.
[310] Ibid.
[311] Australian Competition and Consumer Commission, *Final Report of the Digital Platforms Inquiry,* 366, citing Michael-Ross Fiorento, 'France Passes Controversial "Fake News" Law', *Euronews* (online, 22 November 2018) <https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law>.
[312] Ibid.
[313] Twitter, 'Reporting False Information in France', *Help Center General Guidelines and Policies* (Web page) <https://help.twitter.com/en/rules-and-policies/france-false-information>.

Specialist bodies

Monitoring and awareness

179. The EEAS East Stratcom Task Force was established in 2015 to 'address Russia's ongoing disinformation campaigns'.[314] It was established as part of the response to the European Council's conclusions in March 2015, as set out by the *Action Plan of Strategic Communication*.[315] The EEAS East Stratcom Task Force's objective is to forecast, address and respond to Russia's disinformation campaigns affecting the EU.[316]

180. The EEAS East Stratcom Task Force uses data analysis and media monitoring in 15 languages to identify, compile and expose disinformation cases from Kremlin-aligned media sources spread across the EU, its Eastern Partnership countries (Azerbaijan, Belarus, Georgia, Moldova and Ukraine), the Balkans and the EU's Southern neighbourhood (Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine, Syria and Tunisia).[317]

181. These cases are collected in the 'EUvsDisinfo Database', a searchable open-source repository that currently presents over 65,000 examples of pro-Kremlin disinformation.[318] In the first half of 2019 alone, the EEAS East Stratcom Task Force detected and exposed 1000 cases.[319] 'EUvsDisinfo' is the EEAS Stratcom Task Force's flagship program which intends to increase public awareness and understanding of disinformation operations and campaigns and increase resistance to digital information and media manipulation.[320] Specifically, it publishes materials which seek to spread awareness among the population of disinformation and the methods and practice of its dissemination, as well as educational materials specifically on disinformation which targets elections. It also provides civil society and government outreach.[321]

Policy development

182. In January 2018, the Commission set up the EU High-level Group on Online Disinformation to advise on policy initiatives to counter the dissemination of 'fake news' and disinformation online, culminating in a final report.[322] Subsequently, in April 2018, the Commission announced principles and objectives to guide public awareness about

[314] European Commission, 'Questions and Answers about the East StratCom Task Force' (Web page, 5 December 2018) <https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en>.
[315] General Secretariat of the European Council, *Meeting Conclusions* (Brussels, 20 March 2015, EUCO 11/15, CO EU 1, Conclusion 1) <https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf>.
[316] European External Action Service's East Strategic Communication Task Force, 'About', *EUvsDisinfo* (Web page) <https://euvsdisinfo.eu/about/>.
[317] Ibid.
[318] Ibid.
[319] European Commission, 'Action Plan Against Disinformation: Report on Progress (Progress Report, June 2019) 2 <https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf>.
[320] European External Action Service's East Strategic Communication Task Force, 'About', *EUvDisinfo* (Web page) <https://euvsdisinfo.eu/about/>.
[321] Ibid.
[322] Independent High-Level Group on Fake News and Online Disinformation, *A Multi-Dimensional Approach to Disinformation* (Report, March 2018).

disinformation as well as the measures that the Commission will take.[323] The Commission also developed an *Action Plan Against Disinformation*.[324]

Research and analysis

183. In November 2018, the Social Observatory for Disinformation and Social Media Analysis (**SOMA**) was launched. This project, currently in operation until April 2021, seeks to provide 'a springboard for the social media sector to steer an understanding of its dynamics and the relationship between social media and other sectors'.[325] The objectives and deliverables of SOMA are to:

    (a) map European social media actors by using an open community-based mapping service;

    (b) establish a European centre for social media stakeholders undertaking research on disinformation;

    (c) develop a Source Transparency Index to immediately verify sources;

    (d) consider key solutions, including a platform for content verification, fact-checking tools and social media mapping and visualisation tools for the engagement of European Social Media Innovation initiatives and EU projects;

    (e) develop a methodology for the socio-economic impact assessment of disinformation;

    (f) provide strategies and actions to increase media literacy, analyse legal roadblocks and community-based self-regulation aspects;

    (g) provide policy recommendations based on the analysis of the information collected by SOMA;

    (h) develop tools for community-mapping and an analysis of a future hyper-connected society; and

    (i) create a repository of disinformation-related knowledge.[326]

Code of Practice on Disinformation

184. In late 2018, and in lead up to the European Parliament elections in 2019, the Commission adopted 'conclusions on securing free and fair European elections',[327] and developed the *Code of Practice on Disinformation* (**Code of Practice**).[328] The conclusions included measures such as:

---

[323] European Commission, 'Tackling Online Disinformation: A European Approach' (Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 26 April 2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN>.
[324] European Commission, 'Action Plan Against Disinformation' (Fact Sheet, March 2019) <https://eeas.europa.eu/sites/eeas/files/disinformation_factsheet_march_2019_0.pdf>.
[325] European Commission, 'Social Observatory for Disinformation and Social Media Analysis' (Fact sheet) <https://cordis.europa.eu/project/id/825469>.
[326] Ibid.
[327] European Commission, 'Securing Free and Fair European Elections: Council Adopts Conclusions' (Press Release, 19 February 2019) <https://www.consilium.europa.eu/en/press/press-releases/2019/02/19/securing-free-and-fair-european-elections-council-adopts-conclusions/>.
[328] European Commission, 'EU Code of Practice on Disinformation' (2018) <https://ec.europa.eu/digital-<single-market/en/news/code-practice-disinformation>.

(a) setting up a Rapid Alert System where national contact points in member states can share information rapidly on disinformation campaigns;

(b) strengthening the European media ecosystem, for instance by facilitating the establishment of a network of multidisciplinary independent fact-checkers and academic researchers to detect and expose disinformation across different social networks and digital media;

(c) increasing citizens' resilience by promoting and supporting media and digital literacy;

(d) assessing cyber threats in the electoral context and envisaging measures to address them and preserve the integrity of the electoral system; and

(e) calling on the private sector to invest in resources to deal with election-related online activities in a responsible and accountable manner.[329]

185. The Code of Practice was the first of its kind globally whereby industry agreed on a voluntary basis to self-regulatory standards to fight disinformation.[330] The Code of Practice sets out wide ranging commitments: 'from transparency in political advertising to the closure of fake accounts and demonetization of purveyors of disinformation'.[331] It includes an annex which identifies best practice that signatories should apply to implement the Code of Practice's commitments.[332]

186. To date, the Code of Practice has been signed by Facebook, Google, Twitter, Mozilla, and Microsoft, as well as by advertisers and advertising industry.[333] These platforms and trade associations submitted roadmaps to implementation and were also required to submit a baseline report in January 2019 setting out the state of play of the measures taken to comply with their commitments under the Code of Practice.[334]

187. For the five months leading up to the European Parliament elections, a more targeted monitoring of the implementation of the commitments by Facebook, Google and Twitter was undertaken. Namely, the Commission asked the these platforms to report each month on the actions undertaken to improve scrutiny of advertisement placements, ensure transparency of political advertising and to address fake accounts and malicious use of bots. The reports received for these five months were published alongside the Commission's assessment.[335]

Rapid Alert System

188. The Rapid Alert System (**RAS**), established in March 2019, is a key element of the Commission's *Action Plan Against Disinformation*.[336] This platform facilitates real time communication between EU Member States and institutions on disinformation. There are 28 national contact points, who can, based on agreed criteria, issue alerts on the disinformation campaigns and use the platform to coordinate responses. The platform

[329] Ibid.
[330] European Commission, 'Code of Practice of Disinformation' (News Article, 26 September 2018) <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.
[331] Ibid. See European Commission, 'EU Code of Practice on Disinformation' (2018) cl II.
[332] European Commission, 'EU Code of Practice on Disinformation' (2018) annex II.
[333] European Commission, 'Code of Practice of Disinformation' (News Article, 26 September 2018) <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.
[334] Ibid.
[335] Ibid.
[336] European Commission, 'A Europe That Protects: EU Reports on Progress in Fighting Disinformation ahead of European Council' (Press Release, 14 June 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2914>.

is also used to facilitate sharing of data, insights and best practices between its participants to 'enable common situational awareness, and the development of common responses, as well as ensuring time and resource efficiency'.[337]

Media literacy

189. Many of the EU's measures and initiatives explained above include media literacy components and public awareness about the existence and prevalence of disinformation campaigns. In addition to this, in March 2019, the Commission ran its first European Media Literacy Week with 320 events across Europe.[338]

Action Plan on Democracy

190. The Commission has indicated that it is designing the *European Democracy Action Plan*. Its focus will be broader than fighting disinformation, but will include a plan to strengthen the media sector, create more accountability for platforms and bolster protections for democratic processes.[339] The starting point of the *European Democracy Action Plan* is that to achieve 'a healthy, balanced use of technology' some degree of regulation of the platforms is required.[340]

191. One of the issues to be addressed in this context includes political advertising.[341] Namely, it is intended that the *European Democracy Action Plan* will seek to rectify the lack of legal clarity around political advertising, particularly as it relates to precise targeting based on behaviour, as well as address the lack of transparency on how content is channelled to users and who owns the algorithms.[342] The *European Democracy Action Plan* is anticipated to also address 'the issues of media freedom and media pluralism, access to data by researchers and foreign interference'.[343]

[337] European Parliament, *Parliamentary Questions*, 6 June 2019, (Question P-001705/2019 Vice-President Mogherini on behalf of the European Commission) <https://www.europarl.europa.eu/doceo/document/P-8-2019-001705-ASW_EN.html>.
[338] European Commission, 'Action Plan Against Disinformation: Report on Progress' (Progress Report, June 2019) 4 <https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf>.
[339] Věra Jourová, 'Opening Speech' (Speech, Disinfo Horizon: Responding to Future Threats Conference, 30 January 2020) 2 <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_160>.
[340] Ibid.
[341] Ibid.
[342] Ibid.
[343] Ibid.