ELECTORAL REGULATION RESEARCH NETWORK/DEMOCRATIC AUDIT OF AUSTRALIA JOINT WORKING PAPER SERIES

FOREIGN INTERFERENCE AND AUSTRALIAN ELECTORAL SECURITY IN THE DIGITAL ERA[1]

Dr Melissa-Ellen Dowling

(University of Adelaide)

WORKING PAPER NO. 74 (MAY 2021)

[1] Views expressed in ERRN publications are those of its author(s) and do not necessarily reflect those of the Victorian Electoral Commission, the New South Wales Electoral Commission or the University of Melbourne.

Key Summary

- Australia's federal elections are relatively secure from hard cyber security risks due to digital-analogue hybridity in electoral processes.
- Analogue processes protect preference articulation from digital data manipulation.
- However, Australia's federal elections are vulnerable to soft cyber security risks due to the prevalence of digital disinformation.
- Disinformation has the potential to distort the preference formation and agenda-setting phases of democratic deliberation.
- Interference in elections, or even a widespread perception of interference, can diminish the legitimacy of electoral outcomes.
- Disinformation has the potential to erode social cohesion and jeopardise democratic values that define Australia's political system.

Digitisation of elections in Australia induces new vulnerabilities that malign foreign entities can exploit to subvert our democratic sovereignty. Problems such as inauthenticity, data insecurity, and disinformation are amplified in today's epoch of 'digital era governance.'[2] Following the global trend, Australian elections are digitising: electronic ballots, electronic certified lists, electronic scrutiny and electronic data are rapidly becoming part of the status quo, though the extent of digitisation varies across state and federal jurisdictions.[3] Despite this threat landscape, Australia's digital-analogue hybridity safeguards federal elections from hard cyber security risks (e.g. hacking) that might seek to directly tamper with votes and data. However, elections are vulnerable to soft cyber risks (e.g. information operations). The electoral system's core weakness lies in the time and space between elections: in this period, malign foreign entities (MFEs) can exploit deliberation in the public sphere due to its open circulation of information which they can manipulate with digital disinformation.

Consequently, Australia is relatively secure in terms of preference articulation (voting), but vulnerable during phases of preference formation and agenda-setting (deciding what issues matter, and who and what to vote for). Although Australian legislation designed to counter foreign interference has been enacted, current policy struggles to address the problem of disinformation or account for the covert nature of foreign interference. To ensure Australia remains resilient in the face of foreign interference we should: retain the digital-analogue hybrid system, continue investing in electoral integrity bodies, seek to inoculate society against disinformation, and impose clearer and more stringent liability on internet content hosts for user-generated content identified as disinformation.

Digitisation and Foreign Interference

As democracies around the world digitise election infrastructure,[4] malign foreign entities **(MFEs)** increasingly exploit these newfound opportunities to the detriment of democratic nations. While foreign interference in elections is nothing new, digitisation of governance

[2] Mark Evans et al., "Towards digital era governance: lessons from the Australian experience," in *A Research Agenda for Public Administration* (Edward Elgar Publishing, 2019).

[3] "Electronic Voting at Federal Elections," Parliament of Australia, 2016, accessed 8 Spetember 2020, https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/ElectronicVoting; Joint Standing Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election and Matters Related Thereto*, Parliament of Australia (2018), https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024085/toc_pdf/Reportontheconductofthe2016federalelectionandmattersrelatedthereto.pdf;fileType=application%2Fpdf.

[4] UN, *United Nations E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development*, United Nations Department of Economic and Social Affairs (2020), https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey.

amplifies problems such as **inauthenticity**, **data insecurity**, and **disinformation**. Not only has it become more efficient to interfere in elections with the advent of electronic voting platforms, email, and digital databases, but widespread interference targeted at manipulating voters' preferences is easier than ever due to the rise and prevalence of social media, digital data, and the 24-hour news cycle.[5]

Interference in the 2016 US presidential election forced the issue into the limelight as the Russian government orchestrated a sophisticated electronic assault on US democracy.[6] Exhibiting the hallmarks of information warfare, interference targeted the very fabric of US political culture. The US case signalled the extent to which such interference has the potential to significantly undermine democracy – it highlighted for the first time the extent to which digitisation can engender systemic weakness in a global superpower and bastion of democracy. And, in 2018, the Cambridge Analytica scandal exposed the practice of data-driven political campaigning and microtargeting of electors by non-state actors. Despite the public outcry at the harvest and exploitation of individuals' data, similar operations continue to run deceptive digital campaigns to reshape electors' preferences and/or control voter turnout.[7] Clearly, digital manipulation of elections is not a problem that will abate in the foreseeable future.

While Australia has yet to experience foreign interference at the same scale as the US or the UK, it remains at risk and countering foreign interference has become a strategic priority for the Australian government.[8] Incidents such as the 2019 parliamentary network hacking and foreign financing of political parties demonstrate that Australia is not immune to the foreign interference problem.[9] The Australian presence of data analytics companies and data-driven political consultancies further confirms that vigilance and a defensive approach to safeguarding elections is required since non-state actors continue to profit from the acquisition and use of data for political purposes.[10]

Preference Articulation

Because MFEs may aim to engineer an election outcome, understanding the points of vulnerability in the decision-making process is crucial in order to prevent MFEs from succeeding in this regard.

There are two overarching components to decision-making that are particularly relevant for the foreign interference problem and elections: inputs and outputs. **Inputs** refer to phases of the process within which the public engages in discourse to bring attention to an issue (agenda-setting), along with the stage in which individuals form policy or candidate preferences (preference formation).[11] Preference articulation is the point at which one would vote and thus

[5] Michael L Miller and Cristian Vaccari, "Digital threats to democracy: comparative lessons and possible remedies," *The International Journal of Press/Politics* (2020).

[6] Elizabeth Anne Bodine-Baron et al., *Countering Russian social media influence* (RAND Corporation Santa Monica, 2018); Robert S Mueller, *The Mueller report: Report on the investigation into Russian interference in the 2016 presidential election* (WSBLD, 2019).

[7] Vian Bakir, "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting," *Frontiers in Communication* 5 (2020).

[8] "Countering Foreign Interference," 2020, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference.

[9] Graeme Orr and Andrew Geddis, "Islands in the Storm? Responses to Foreign Electoral Interference in Australia and New Zealand," *Election Law Journal: Rules, Politics, and Policy* (2020).

[10] See e.g. Isabel Dayman, "SA Premier denies deliberate data collection through Liberal Party's NationBuilder campaign software," *ABC News* 2 April 2021 2021, https://www.abc.net.au/news/2021-04-01/sa-premier-says-no-data-deliberately-collected-by-campaign-tool/100044538.

[11] Vivien Schmidt and Matthew Wood, "Conceptualizing throughput legitimacy: Procedural mechanisms of accountability, transparency, inclusiveness and openness in EU governance," *Public Administration* 97, no. 4

communicate preferences to government. Inputs contribute towards an electoral **output**, in turn generating an outcome. If MFEs are able to influence the inputs through manipulation of Australia's mechanisms of public participation in politics, they gain power relative to domestic actors and can diminish national sovereignty and/or reduce the perceived legitimacy of participatory processes and institutions.

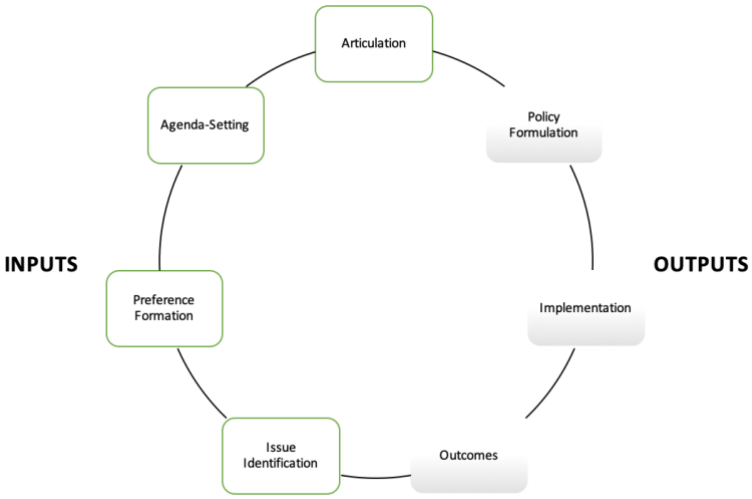

Figure 1: Decision-making circuit. Adapted from Birkland.[12]

Fortunately, directly influencing an election output in Australia is difficult due to stringent hybrid digital-analogue mechanisms which safeguard voting processes from the digital problems of inauthenticity and data (in)security.

Digital-Analogue Hybridity

Where digitisation presents potential risks, analogue processes mitigate those risks. For example, although electronic mechanisms are becoming increasingly incorporated into the Australian electoral system and might introduce risks associated with data security, voting in federal elections is still characterised by predominantly analogue processes.[13] Paper-based voting systems render significant digital interference difficult:[14] the inauthenticity problem is diminished through onsite manual identity verification, and the data security problem is alleviated (though not entirely removed) by the possibility of cross-checking and auditing data with manual ballots and records.[15] There is also a human-centric approach to the use of

(2019); Vivien A Schmidt, "Institutionalism," *The Encyclopedia of Political Thought* (2014); Thomas A Birkland, *An introduction to the policy process: Theories, concepts, and models of public policy making* (Routledge, 2019).

[12] Birkland, *An introduction to the policy process: Theories, concepts, and models of public policy making*.

[13] Note that e-voting has been widely implemented in state elections and it has been trialled at the federal level. Aspects of federal elections aside from ballot casting have been digitised but are still subject to human oversight (e.g. 2016 election AEC scanning of Senate ballots using Fuji Xerox Document Management Services): see for example, Lundie, "Electronic Voting at Federal Elections."; "iVote," 2020, accessed 12 August 2020, https://www.elections.wa.gov.au/ivote; "iVote," 2020, accessed 12 August 2020, https://www.elections.nsw.gov.au/Voters/Other-voting-options/iVote-online-and-telephone-voting.".

[14] Intelligence Security Committee, *Russia Report* (2020), https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl.

[15] Joint Standing Committee on Electoral Matters, *Second Interim Report on the Inquiry into the Conduct of the 2013 Federal Election: An assessment of electronic voting options*, Parliament of Australia (2014), https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22publications/tabledpapers/b2a871d0-8106-42e3-8481-8749744020e7%22; Joint Standing Committee on Electoral Matters, *Report on the Conduct of the 2016 Federal Election and Matters Related Thereto*.

electronic election technology in Australia which potentially reduces the risks of inauthenticy and data insecurity. For example, while the AEC implemented scanning of senate ballots in the 2016 federal election, this process reportedly involved significant human oversight.[16] Further, given the use of paper ballots, any discrepancies in the digital record could hypothetically be cross-checked in the event of a contested electoral outcome. This shows that it is possible to balance digitisation with analogue methods to optimise electoral security.

The conduct of the Western Australian 2013 senate election illustrates the value of analogue mechanisms for maintaining electoral integrity. In that case, a recount of the ballot papers was required due to a close margin and it was discovered that approximately 1,000 ballot papers were missing. The election was therefore contested via the Court of Disputed Returns, and the Court ordered a redo of the election.[17] This state-level example shows that if there are grounds to dispute an election, the Australian system has functional avenues to do so. The example, though not a foreign interference situation, indicates that if there were widespread suspicions of interference (irrespective of whether it has occurred), the potential erosion of trust in government and the system that might occur from the perception of interference can be prevented, or at least mitigated, by contesting the results and a verifiable recount.

Perceptions of Interference

Despite the protections built into Australia's democratic processes, the legitimacy of election results can nevertheless be undermined if there is public perception of a compromised input process. This is irrespective of whether interference has actually occurred, hence the necessity of retaining mechanisms for transparently tracking, validating, and demonstrating the integrity of the process to the public.

The public sphere is therefore vulnerable since it is within the discursive space that information is circulated. It is also the area in which existing foreign interference policy is struggling to regulate, partly because robust regulation of the public sphere contravenes the tenets of democracy; a reminder of democracy's fundamental weakness in information warfare.[18]

Preference Formation

Influencing election outputs through disinformation is therefore a serious concern because it can reshape organic public inputs into the decision-making process. This indicates that while the preference articulation phase of participatory processes is largely secure from direct tampering or 'hard' cyber threats, the preference formation and agenda-setting phases are vulnerable to MFE interference and can distort election outcomes.

Interference that targets people before they cast a ballot is very difficult to detect, let alone counter. It affects what people think they want, which in turn will affect what they contribute to the participatory process – their input will reflect their interests, and their interests might be influenced by MFEs' disinformation campaigns. Indeed, this remains a divisive issue with respect to the UK's Brexit referendum – to what extent did Russian disinformation affect the result?[19] Interference that corrupts organic preference-shaping mechanisms guarantees a

[16] Lundie, "Electronic Voting at Federal Elections."
[17] "The disputed 2013 WA Senate election," Parliament of Australia, 2013, https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2013/November/The_disputed_2013_WA_Senate_election.
[18] Laura Rosenberger and Lindsay Gorman, "How Democracies Can Win the Information Contest," *The Washington Quarterly* 43, no. 2 (2020).
[19] Intelligence Security Committee, *Russia Report*.

distorted election result.

However, MFEs' goals are not always directed at achieving a specific election result. Sometimes, the apparent aim is to destabilise a nation to create further vulnerabilities. Disinformation therefore also manifests as an acute concern for Australian democracy for its potential to diminish social cohesion. Discourse associated with elections and other national voting events such as referendums create opportunities for polarising discourse that has the capacity to exacerbate tension within society. Take for example, the Marriage Equality Survey of 2017: its very structure presented the issue in a binary manner with a 'yes' or 'no' vote required and it generated considerable polarised debate in the public sphere.[20] MFEs can capitalise on existing and endemic polarisation to increase societal fissures and weaken pillars of liberal democracy such as tolerance, inclusion, equality, and trust.[21] We saw such dynamics in the US where Russian disinformation operations reportedly fuelled protest activity without an allegiance to a particular side.[22]

Current Policy and Regulation

- Although Australia is developing a robust regulatory framework to protect democratic institutions from foreign interference (see figure 2), the extent to which legislative initiatives are effective is unknown and requires further investigation.
- Existing policy also struggles to address the deeper concern of disinformation targeted towards the public.
- By its very nature interference is covert and difficult to identify,[23] meaning that the likelihood of legislation that criminalises foreign interference having either deterrent or punitive effects is questionable. The cyber attribution problem is a particularly significant barrier to effective regulation of digital disinformation. Identification of producers of disinformation is not only challenging, but in the majority of cases it is impossible. The transnationality of the digital space, use of virtual private networks, and difficulty of unequivocally proving a state actor's culpability given use of third-party contractors makes combatting cyber warfare enormously difficult. In light of such challenges, we are increasingly seeing debate about imposing liability on internet content hosts for user-generated content.[24] This is a rapidly evolving area of law within which we can expect to see ongoing changes.
- Bodies such as the Australian Electoral Commission (AEC) and the Electoral Integrity Assurance Taskforce focus on maintaining electoral integrity, and ASIO's Counter Foreign Interference Taskforce works towards mitigating foreign interference more broadly.
- The AEC contributes towards secure federal elections by overseeing and administering

[20] Australian Bureau of Statistics, *Report on the Conduct of the Australian Marriage Law Postal Survey*, ABS (2017).
[21] For components of liberal democracy, see e.g. Robert A Dahl, *On democracy* (Yale university press, 2008).
[22] House Committee on Oversight and Reform, "National Security Subcommittee Seeks Classified Briefing on Foreign Interference in Racial Justice Protests," news release, June 16 2020, 2020, https://oversight.house.gov/news/press-releases/national-security-subcommittee-seeks-classified-briefing-on-foreign-interference; Mueller, *The Mueller report: Report on the investigation into Russian interference in the 2016 presidential election*.
[23] Melissa-Ellen Dowling, "Democracy under Siege: foreign interference in a digital era," *Australian Journal of International Affairs* (2021) ahead of print. DOI: https://doi.org/10.1080/10357718.2021.1909534.
[24] Chris Marsden, Trisha Meyer, and Ian Brown, "Platform values and democratic elections: How can the law regulate digital disinformation?," *Computer Law & Security Review* 36 (2020); Majid Yar, "A failure to regulate? The demands and dilemmas of tackling illegal content and behaviour on social media," *International Journal of Cybersecurity Intelligence & Cybercrime* 1, no. 1 (2018); Petros Iosifidis and Leighton Andrews, "Regulating the internet intermediaries in a post-truth world: Beyond media policy?," *International Communication Gazette* 82, no. 3 (2020).

stringent voting procedures in line with the Commonwealth Electoral Act 1918 (Cth).

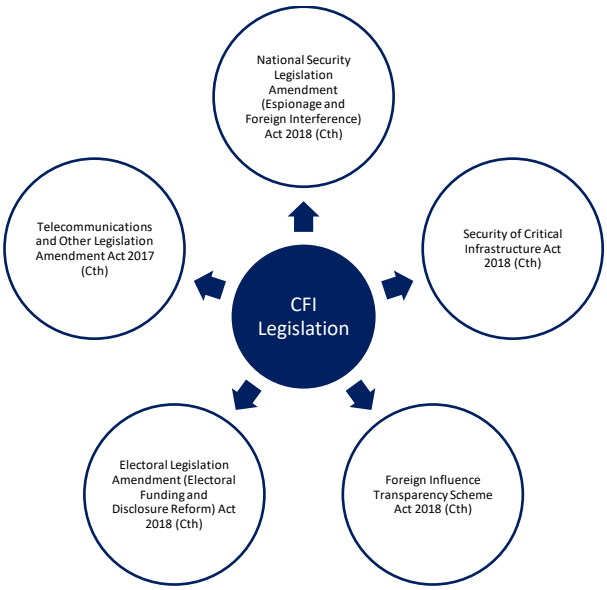

Figure 2: Countering Foreign Interference legislation

Policy Recommendations

- **RESIST** rolling out e-voting at the federal level. Since digital-analogue hybridity is a strength of Australia's participatory processes we should continue to operate certain electoral processes using a hybrid model. Retention of paper ballots and analogue ballot storage is essential. However, there is no reason why digital technology cannot be deployed for less high-stakes processes that constitute less risk in terms of the articulation of preferences (e.g. use of electronic certified lists).
- **INVEST** in bodies that promote the integrity of elections since maintaining the integrity of democratic processes is paramount to countering foreign interference and building democratic resilience. Human oversight of digital processes is essential.
- **INOCULATE** society against disinformation. Since disinformation presents as the most acute concern we should educate regarding disinformation.
- **REGULATE** internet content hosts by imposing liability on internet intermediaries for user-generated content that is identified as disinformation. Since the human sources of disinformation are rarely identifiable, platform regulation might be the only realistic recourse and means of mitigating the political harm of disinformation. The scope and nature of such liability forms the subject of contemporary debate.[25]

Note

This brief is a modified version of Dowling, M.E, "The Digital Dilemma: Countering Foreign Interference." *The Stretton Institute*, 3 November, 2020, https://www.adelaide.edu.au/stretton/news/list/2020/11/03/the-digital-dilemma-countering-foreign-interference.

[25] See note 23.

References

Australian Bureau of Statistics. *Report on the Conduct of the Australian Marriage Law Postal Survey.* ABS (2017).

Bakir, Vian. "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting." *Frontiers in Communication* 5 (2020): 67.

Birkland, Thomas A. *An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making.* Routledge, 2019.

Bodine-Baron, Elizabeth Anne, Todd C Helmus, Andrew Radin, and Elina Treyger. *Countering Russian Social Media Influence.* RAND Corporation Santa Monica, 2018.

Dahl, Robert A. *On Democracy.* Yale university press, 2008.

Dayman, Isabel. "Sa Premier Denies Deliberate Data Collection through Liberal Party's Nationbuilder Campaign Software." *ABC News* 2 April 2021 2021. https://www.abc.net.au/news/2021-04-01/sa-premier-says-no-data-deliberately-collected-by-campaign-tool/100044538.

"Countering Foreign Interference." 2020, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference.

Dowling, Melissa-Ellen. "Democracy under Siege: Foreign Interference in a Digital Era." *Australian Journal of International Affairs* (2021): 1-5. Ahead of print. DOI: https://doi.org/10.1080/10357718.2021.1909534.

Evans, Mark, Patrick Dunleavy, Carmel McGregor, and Max Halupka. "Towards Digital Era Governance: Lessons from the Australian Experience." In *A Research Agenda for Public Administration*: Edward Elgar Publishing, 2019.

House Committee on Oversight and Reform. "National Security Subcommittee Seeks Classified Briefing on Foreign Interference in Racial Justice Protests." news release, June 16 2020, 2020, https://oversight.house.gov/news/press-releases/national-security-subcommittee-seeks-classified-briefing-on-foreign-interference.

Intelligence Security Committee. *Russia Report.* (2020). https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl.

Iosifidis, Petros, and Leighton Andrews. "Regulating the Internet Intermediaries in a Post-Truth World: Beyond Media Policy?". *International Communication Gazette* 82, no. 3 (2020): 211-30.

Joint Standing Committee on Electoral Matters. *Report on the Conduct of the 2016 Federal Election and Matters Related Thereto.* Parliament of Australia (2018). https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024085/toc_pdf/Reportontheconductofthe2016federalelectionandmattersrelatedthereto.pdf;fileType=application%2Fpdf.

———. *Second Interim Report on the Inquiry into the Conduct of the 2013 Federal Election: An Assessment of Electronic Voting Options.* Parliament of Australia (2014). https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22publications/tabledpapers/b2a871d0-8106-42e3-8481-8749744020e7%22.

"The Disputed 2013 Wa Senate Election." Parliament of Australia, 2013, https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2013/November/The_disputed_2013_WA_Senate_election.

"Electronic Voting at Federal Elections." Parliament of Australia, 2016, accessed 8 Spetember 2020, https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/ElectronicVoting.

Marsden, Chris, Trisha Meyer, and Ian Brown. "Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation?". *Computer Law & Security Review* 36 (2020): 105373.

Miller, Michael L, and Cristian Vaccari. "Digital Threats to Democracy: Comparative Lessons and Possible Remedies." *The International Journal of Press/Politics* (2020): 333-56.

Mueller, Robert S. *The Mueller Report: Report on the Investigation into Russian Interference in the 2016 Presidential Election.* WSBLD, 2019.

"Ivote." 2020, accessed 12 August 2020, https://www.elections.nsw.gov.au/Voters/Other-voting-options/iVote-online-and-telephone-voting.

Orr, Graeme, and Andrew Geddis. "Islands in the Storm? Responses to Foreign Electoral Interference in Australia and New Zealand." *Election Law Journal: Rules, Politics, and Policy* (2020).

Rosenberger, Laura, and Lindsay Gorman. "How Democracies Can Win the Information Contest." *The Washington Quarterly* 43, no. 2 (2020): 75-96.

Schmidt, Vivien A. "Institutionalism." *The Encyclopedia of Political Thought* (2014): 1836-39.

Schmidt, Vivien, and Matthew Wood. "Conceptualizing Throughput Legitimacy: Procedural Mechanisms of Accountability, Transparency, Inclusiveness and Openness in Eu Governance." *Public Administration* 97, no. 4 (2019): 727-40.

UN. *United Nations E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development.* United Nations Department of Economic and Social Affairs (2020). https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey.

"Ivote." 2020, accessed 12 August 2020, https://www.elections.wa.gov.au/ivote.

Yar, Majid. "A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media." *International Journal of Cybersecurity Intelligence & Cybercrime* 1, no. 1 (2018): 5-20.