# ASPG Conference –
# Parliaments Navigating Disruption in 2019

# Using civic technology to engage citizens


## Hon Jonathan O'Dea MP
## Speaker, NSW Parliament


## Use of civic technology

Technology is a great disrupter and will continue to be increasingly in the future. This paper looks at civic technology - what it means and how it is used to engage citizens, in both an international and NSW context. It looks at its positive impacts and some challenges with its use. Civic technology is technology that enables greater citizen participation and engagement with government services and public decision making. It improves the relationship between government and people by enhancing communications and facilitating political exchange. This can include government operated online platforms where citizens can vote on policy or propose new ideas.

It has the potential to change the way politics is conducted worldwide by enabling greater efficiency of government services, expanding the role of digital tools, and enhancing citizen powered democracy. The positive transformative potential of civic technology is undeniable. However, in disrupting the status quo, it can also have negative impacts eg. relating to cyber security and the potential to undermine democratic processes in countries that use it.

Over the last decade, civic technology has been increasingly adopted by governments across the globe. It has taken many forms and provided a range of benefits. For

example, it empowers Parliaments to better engage with disadvantaged communities through mobile technologies such as tablets and smartphones. Many people can better participate in e-democracy methods through e-surveys, internet voting, and improved interaction with government services such as digital drivers licences and passports. For example, the ‘Service NSW’ online platform enables customers to submit, view, vote for, and receive feedback on ideas (Service NSW 2017). They have also proposed digital licences (including drivers licences) via an app, with a launch date now scheduled for late 2019 (Service NSW 2019). With a ‘MyServiceNSW’ account login, citizens have also recently been able to vote for a My Community Project under a NSW government initiative to fund local projects proposed by citizens. The online platform allowed citizens to rate the importance of these projects to improve the wellbeing of people and communities in each electorate. The NSW Government is now investing millions of dollars into these citizen-led projects.

Civic technology is further being used to provide maps of civic activity and artificial intelligence (AI) for machine learning, predictive text and natural language generation. An example of AI use by governments is the Singapore Government creating chatbots, functioning as digital representatives for particular citizen services. These chatbots field questions from citizens and provide relevant answers. In another example, the Mexican Government has proposed an initiative to use algorithms to automatically classify citizen petitions and send them to the correct offices (Mehr 2017).

While civic technology offers a range of benefits, perhaps the most significant is its ability to enable greater participation in democracy. According to Dubow (2017), civic technology has lowered the barriers for civic engagement and enabled direct

participation in decision making, including by people whose engagement has traditionally been lower. However, some academics have questioned whether civic technology substantially enhances the democratic process, or whether it essentially just provides another platform for people who are already politically informed to voice their opinions.

Other concerns also exist e.g. that civic technology may further entrench disadvantage for the elderly and people without reliable access to the internet, or the skills to use it. It also can give the state greater power to track and report citizen behaviour. For example, the NSW Government uses a digital fare system for public transportation called 'Opal' cards that allows tracking of citizen location and movement. Arguably, this impinges on personal privacy, with potentially dangerous consequences if information is leaked. Other notable examples include China's face recognition system, the access authorities have to private mobiles, and close monitoring and surveillance of web searches.

Despite its use by Parliaments and governments, civic technology has not been utilised to its maximum potential. There are multiple types of civic technology in a highly fragmented sector, ranging from technology used by state governments to improve services, to citizen initiated forums. Arguably, insufficient public participation and limited mainstream media coverage have hindered its growth (Field 2016). Some types of civic technology such as internet voting have also been disregarded by many Parliaments due to scepticism concerning security and reliability. Similarly, while civic technology exists in many nations, it is not always used effectively. For example, civic

technology in some nations is used to promote a façade of citizen powered democracy. Some of these issues will be further explored later.

## Digital tools Internationally

Citizen deliberation software is currently being used by different levels of government around the world to encourage citizens to engage with the democratic process. These digital platforms help assess the views of citizens on potential legislative and social change, as well as on budget decisions. Examples include e-petitions, surveys, polling, online communities and platforms where debates take place on policy and budgets. Such tools are helping to restore citizens' trust in the legitimacy of political institutions, and making politics relevant to more people (Copeland 2017). These online platforms can be viewed as an extension to the broader public sphere, and are delivering positive political change. However the situation is complex, with some governments arguably using these platforms as a manipulative tool, rather than sincerely engaging with the public e.g. with China's control of local internet and monitoring of online activity.

There are various jurisdictions where these tools have already operated. In 2014, Taiwanese citizens initiated 'vTaiwan', which later became a collaboration with the government. The platform was created with the intention of engaging experts and relevant members of the public on various issues. It allows for a dialogue between diverse groups, and over 80% of cases discussed have led to decisive government action. For example, vTaiwan helped pass the FinTech Sandbox Act, that empowers the financial tech field to conduct transparent and accountable experiments. Belgium enacted a similar platform in Brussels called 'OpenWall', by engaging citizens,

companies, governments, and innovators in political discussion, in order to raise policy and societal issues. For example, policy issues have been raised to improve urban public spaces and distribute kits to schools to monitor soil and air pollution (Garrigues 2017).

Similarly, ‘Decide Madrid’ is an initiative led by the Madrid City Council allowing citizens to discuss issues, vote on policy, engage in participatory budgeting, and propose new ideas (DeJohn 2017). Proposals that gain the support of at least 1% of the population are put to a binding public vote. The council must then evaluate the legality and cost of successful proposals within a month. It is one of their most successful projects to date, receiving the 2018 ‘UN Public Service Award’ for establishing open, transparent, participatory, and inclusive government models (NIMD 2018).

In Iceland, an online platform called ‘Betri Reykjavik’ was created for citizens to inform each other on political issues and submit policy proposals. Each month the city council evaluates the top proposals and issues a response. The ideas are accessible to the public and can be debated on the site. Citizens are then encouraged to cast a vote for or against each proposal (Lackaff 2016). Highlighting its immense success, more than 70,000 people have visited the site out of a population of 120,000 in Reykjavik. Over 800 citizen initiatives have been approved by the city council and it has helped to build confidence in its elected politicians (Bjanarson 2017).

In 2018, the government of Singapore backed ‘Virtual Singapore’, which acts as a collaborative space and is designed to eventually assist in developing smart city

initiatives. One such initiative is to deploy sensors to monitor environment, health and safety conditions. Its stated goal is to engage the public by creating awareness and services that enrich the community, and help businesses collect a wealth of information for resource planning and management (Hartley 2019). Yet another case of successful citizen deliberation is in Toronto, where civic technology cyclists helped create an app to report bike parking issues to the city (Wytze 2018).

Civic technology is not exclusively used by first world nations or democracies. In 2014, Kenya launched 'MajiVoice', a website allowing the public to report complaints regarding water services to water providers. The intention was to improve services and provide citizens with a convenient method of reporting concerns (Belcher & Lopes 2017). Similarly, Estonia established 'Rahvakogu' in 2013 to crowdsource ideas and proposals from the public. The issues covered include Estonia's electoral laws, and the future of democracy in the nation. The proposals were then presented to the Parliament, where 15 of the policies were debated and 7 were implemented (Bjanarson 2017). As a result, Rahvakogu was considered an overwhelming success.

Despite the success of citizen deliberation software internationally, some cases indicate these digital tools are not always effective in delivering positive political change. An example of this is Russia's 'Active Citizen' Platform in Moscow, allowing citizens to vote on non-political city decisions. There are concerns that some online votes were fake (possibly due to bots and AI), that the platform largely avoided important issues, and excluded the public from voicing their own issues (Wytze 2018). China also uses digital tools, but for largely dubious reasons such as monitoring websites and feeding private citizen metadata into AI models to make predictions (Tan

2018). These are examples of how digital tools are sometimes ineffective or used manipulatively by governments, having adverse impact on positive political change.

Civic technology has recently been used by both Australian Prime Minister, Scott Morrison and UK Prime Minister, Boris Johnson to invite public questions through Facebook. These sessions utilise a digital tool to help the leaders appear interested and connected to the concerns of their constituents.

Facebook Australia has hosted a number of Facebook Live sessions with Scott Morrison and other federal Cabinet members. The public are encouraged to post relevant questions on the politicians' Facebook pages. The politicians then select which questions they will answer live on Facebook. Boris Johnson hosted his first 'People's PMQs' in August 2019. During the PMQs (prime minister's questions) he answered questions relating to Brexit, education, infrastructure, knife crime and mental health.

Some people would argue these online forums allow politicians to carefully avoid critical issues by controlling the questions they address. Their answers arguably avoid scrutiny by other politicians or journalists in real time. While bypassing traditional media outlets, politicians know these outlets will probably report on the sanitised media broadcasts if that is the only information released by the government on certain issues.

The NSW Legislative Assembly is currently considering introducing a number of digital reforms, including the introduction of people's questions.

## Changes to process in the NSW Legislative Assembly

The NSW Legislative Assembly wants to improve digital interactions with citizens to help make politics more relevant to more people. Proposed changes might include the introduction of e-petitions, subtitled livestreaming of parliament, and facilitating questions from the public for Parliament's Question Time. E-petitions have already been agreed upon in principle, and will likely require a 20,000 signature threshold to prompt a parliamentary debate, in contrast to the current 10,000 threshold for paper petitions.

The NSW Legislative Assembly currently livestreams parliamentary proceedings from its website, with potential to further expand its reach through platforms such as Facebook. Subtitles enabled by voice recognition technology could soon assist hearing-impaired citizens to engage with their state politicians, for example, on screens in the parliamentary precinct featuring clear subtitles that narrate a day at NSW Parliament.

The concept of a 'public question', where the public can generate questions of state ministers, potentially for Parliament's Question Time, could provide elected Members an opportunity to better digitally engage with their communities. This might be done through Members promoting associated online survey tools or email campaigns to generate public questions. Such developments might help to further engage citizens, although concerns around security of and distortion through digital tools have generated some scepticism around their effectiveness. These arguments are explored further later.

## Ivote

iVote is an online remote voting platform for state elections which began operating in 2011, for voters who were blind or had vision impairment. It has now expanded to include voters who have other disabilities, live more than 20km from a polling place, or will be out of the state on election day. iVote was initiated in NSW, and is a registered trademark of the NSW Electoral Commission. A similar system was introduced by the Western Australia Electoral Commission for the 2017 WA state election, making online and telephone voting available to people enrolled to vote in Western Australia (WA Electoral Commission). As of 2019, NSW and Western Australia are the only states with an online voting platform.

In order to vote online or remotely, eligible people visit the iVote website to apply. They are provided a number within Australia or from overseas, and choose whether to vote online or via telephone. A password must be provided for online voting or a PIN for telephone voting. Once this process is completed, an iVote number is sent to voters through the method they select, including email, SMS or telephone call. That number, combined with the password, is used to cast a vote online using the iVote platform. Finally, a verification app can be downloaded to confirm the vote was recorded (NSW Electoral Commission 2019).

The NSW Electoral Commission has recently faced a number of security and technical issues on the platform. While iVote apparently has not faced any hacking attempts, the NSW Electoral Commission revealed an internal flaw in the system which may leave it vulnerable to attacks. The affected component of the software is called ‘mixnet’, which randomises the order of votes before being counted to ensure they

cannot be connected to individuals. This allows voters to remain anonymous (NSW Electoral Commission 2019). The code did not provide complete verifiability, leaving the system vulnerable for hackers to pass verification and manipulate votes (Hendry 2019). While the software provider corrected the code, this flaw reveals the potential for digital technology to enable vote manipulation.

During the NSW state election in 2015, an internal flaw in iVote was uncovered regarding voting for the NSW Legislative Council. The results were so close that one seat in the Legislative Council may have been decided by hacked votes. Researchers were able to identify flaws in the system that could be used to spy on and modify votes without detection. Before the system was fixed, over 66,000 votes had already been cast online, including 3,177 that decided one seat in the Legislative Council. A year later, under questioning in state parliament the NSW Electoral Commmission admitted there were significant anomalies reported by voters, which they had not been transparent about immediately after the election (Porup 2018). This is another example of how flaws in online voting can lead to external vote manipulation, posing a danger to free and open democratic elections.

Technical issues also affected the platform in the 2019 NSW election. During the election, people who logged in to iVote complained of the site crashing and then being unable to vote. In response, the NSW Electoral Commission confirmed that iVote was offline while the issue was being resolved (Tovey 2019). The site’s inability to handle high levels of traffic led to usability issues that affected public perceptions of the integrity of online voting.

NSW and Western Australia are not the only jurisdictions in the world that use an online voting platform. Similar to iVote, Switzerland uses an e-voting system as part of 'Swiss Post'. Swiss Post e-voting allows Swiss citizens, domestic and abroad, to participate in elections and cast votes through their computer or phone. The process is similar to iVote. A security code is sent to voters by post which they can use to log into the online voting platform. They then cast a vote which is stored in the electronic ballot box. Like iVote, the Swiss system uses the same software supplier, Scytl. Therefore the security issues that were present in iVote appear to affect Swiss Post's e-voting system (NSW Electoral Commission 2019).

In 2011 Gujarat became the first state in India to use internet voting. Similar to Swiss Post e-voting and iVote, Gujarat awarded the contract to Scytl to provide the platform. For the first time, Indians were able to cast their votes from home and over the internet. During the second round of online elections in March 2011, over 77% of registered e-voters cast their votes online (Scytl). The project was considered a success and met with a favourable response.

Despite the increasing use of digital technology by Parliaments, online voting has not been widely accepted. In Spain, several issues have been raised relating to security, voter identification and identity theft. During a referendum in Barcelona, it was revealed that someone had logged on under a prominent candidate's details and voted as him (Verified Voting). France has also faced similar issues regarding security. In 2014, France's first online primary was conducted, but the system was proven simple to breach. It was easy to vote several times under different names, bringing not only the outcome of the election into doubt, but also the use of e-voting technology in

general. The cases outlined have driven concern and scepticism around online voting, thereby discouraging governments from confidently adopting it.

## Cyber security

Leading up to the 2019 Australian federal election, reports emerged of an attempt to infiltrate the Australian Parliamentary network, which is used to exchange emails and store data. Further investigations revealed the attack was sophisticated and likely state-sponsored. The attack relied on malware attached to an email and, once opened, allowed the hackers to infect intranet servers, redirect network traffic to extract data, and place additional malware to maintain control of the infected systems. Despite a lack of evidence, it was speculated by people such as Peter Hartcher (2019), that China coordinated the attack due to a history of cyber attacks against the Australian government, and recent tensions regarding trade. This attack was a major security breach demonstrating the successful infiltration of Parliament and major political parties in the lead up the federal election. However, there is no evidence that any data was leaked (Doche, McCombie & Rabehaja 2019).

In its aftermath, swift action was taken by the Australian Government to prevent the situation recurring. In February 2019, the NSW Government and Government Chief Information Security Officer released the 'NSW Cyber Security Policy'. The Policy introduced mandatory cyber security requirements on all NSW Public Service Agencies (Department of Finance, Services and Innovation [DOFSI] 2019). Importantly, the policy mandates every agency to identify its most valuable systems, and enforce regular cyber security education for all employees, ICT service providers

and contractors (Doche, McCombie & Rabehaja 2019). This will help strengthen the resilience of government agencies against potential cyber attacks in the future.

The UK Parliament faced a similar attack in June 2017, when an unauthorised attempt was made to gain access to the email accounts of politicians. Hackers attempted to retrieve the email passwords of ministers in order to sell them online, specifically targeting accounts with weak passwords. Fortunately, only 90 email accounts were compromised, making up less than 1% of email accounts linked to the Parliament. However, it was treated as a serious security breach that UK British security services noted was likely coordinated by agencies linked to Russia or China (Parliament UK 2017). In the aftermath, the UK Government invested heavily in preventative cyber security measures. An important technological change included increasing multi-factor authentication, by requiring MPs to use two or more pieces of evidence to log in (Parliament UK 2017).

Other cases of state-sponsored cyber security attacks have occurred in recent years. During the lead up to the 2016 US Presidential election, US agencies revealed that Russia hacked and leaked Democratic Party communications, attempting to interfere with the election process. Hackers infiltrated the Democratic National Committee (DNC) computer network, leading to a data breach. The attack resulted in the theft of emails and documents from the DNC, which were released online and likely sent to WikiLeaks (Gass 2016). Cyber security firms indicated that two Russian intelligence agencies coordinated the attack (Sanger & Perlroth 2016). The hackers succeeded in leaking substantial amounts of information to the public (Gass 2016).

Similar to the 2016 US Election, the 2017 French election also experienced a cyber security attack. Several days before the presidential election, data was hacked from Emmanuel Macron's campaign team and released online. The leak involved thousands of emails and was again linked to Russia attempting to interfere in a foreign election. However, the hackers made several mistakes, and the French Government responded well, resulting in a failure to really influence the public (Conley & Vilmer 2018).

With the adoption of digital tools by parliaments around the world, and the growth of online communications, the issue of cyber security has understandably become a priority for governments as they promote democratic processes in their respective nations. However, cyber security breaches have adverse effects on these democratic processes. The US and French cases reveal how foreign actors and states can attempt to manipulate democratic processes through cyber security attacks. Cyber security is therefore a priority to address in promoting a strong and safe digital sphere, and a truly democratic environment.

## A challenge to democracy?

Digital technology has further potential to undermine democratic processes by increasing government power, to the detriment of free speech in the digital sphere. The 2017 French election illustrates this argument. In response to the cyber attack, the government placed pressure on Facebook to suspend 30,000 attacks. However, the number of suspended accounts actually totalled 70,000, in a move seen to be more about greater government control than the prevention of attacks (Conley & Vilmer 2018). While many of the accounts were fake, it is likely that some of the

suspended accounts featured the views of genuine citizens and were inadvertently shut down for anti-government rhetoric.

Around the world, some governments are using digital tools such as social media for censorship, spreading misinformation and silencing dissent, such as the examples given linked to Russia and China. Social media played a key role in the uprising against the Iranian regime in 2009, with the Arab Spring in 2011, and in Ukraine in 2013. In turn, it was perceived as a global force for citizens' emancipation. However, technology is not static and nor is democracy. Authoritarian regimes began cracking down on internet freedom, censoring websites, and hiring hackers and trolls to spread misinformation (Annan 2018). Trolls can also spread conspiracy theories and false narratives, which are more likely to go viral, indicating how social media manipulation has implications for reason-driven dialogue in democracies (Parliament of Australia 2019). However, government control of social media is not limited to authoritarian regimes. After a gunman livestreamed a mass shooting in 2019, Australia passed legislation to regulate social media companies that did not remove violent content. In 2017, Australia also passed a bill requiring internet service providers to store citizens' digital history for two years, which can be accessed without a warrant. This prompts questions of whether social media and digital tools are emancipating citizens, or controlling them.

Digital technology used by governments can also pose dangers to citizens whose personal information may be hacked. In 2018, the personal data of 300,000 people across towns in the US was stolen by hackers. Security agencies showed how vulnerabilities in 'Click2Gov', a government payment software, let hackers onto the

networks to steal credit and debit card data. The victims were citizens using town websites to pay fines, permits and taxes (Roberts 2018).

Similarly, during the French Government's response to the 2017 election hacking, electronic voting abroad was discontinued due to the risk of foreign actors hacking and manipulating citizens' votes. These examples provide insight into the potential dangers associated with citizen use of digital tools provided by governments.

Another danger posed by governments using civic technology includes the strain on public credibility and trust when a façade of democracy is encouraged. An example of this is Russia's 'Active Citizen' Platform in Moscow, allowing citizens to vote on non-political city decisions. As earlier noted, there were concerns over fake votes, and the fact that the platform avoided or prevented important issues being expressed (Wytze 2018). So, civic technology can be used by governments to create the façade of citizen powered democracy, thereby damaging the technology's credibility and reputation.

The impact of civic technology on public trust in the government is complicated. Citizen deliberation software has improved public confidence in elected politicians across Iceland, Spain, Estonia, Taiwan and Singapore (Bjanarson 2017). These tools are helping to restore citizens' trust in the legitimacy of political institutions (Copeland 2017). However, most civic technology projects are confined to cities and states, rather than federal contexts. Therefore, when public trust is repaired in particular cities, it is not necessarily indicative of general public opinion across the nation or globe. So while civic technology has improved engagement and public trust in the government in particular cities, its effect on a larger scale is somewhat unclear.

## Conclusion

Civic technology has spread across the globe, promising citizen powered democracy and greater transparency. While this move has been primarily led by Western nations, states across Asia, Africa and South America are likewise utilising the technology. Civic technology provides both opportunities and challenges. It arguably empowers disadvantaged communities, enables greater efficiency of government services, and encourages greater participation in democracy.

Yet concerns persist, including the argument that civic technology merely provides another platform for people who are already politically informed. Although citizen deliberation software has been adopted by various jurisdictions with success in delivering positive political change, it is not always successful, as in Russia. The issue of cyber security generates scepticism regarding civic technology, while other issues such as foreign election interference, the online spread of misinformation, and increasing government control can all undermine democratic processes.

In response to the growth of civic technology, the NSW Legislative Assembly is improving digital interactions with citizens to make politics relevant to more people. Parliamentary proceedings are currently livestreamed online, and the concepts of ‘public questions’ and e-petitions are being considered. The NSW government also initiated iVote, an online remote voting platform encouraging greater participation in democracy, although it has faced a number of technical and security issues.

Despite its potential drawbacks, civic technology is undoubtedly becoming more relevant to more people. It is therefore crucial for parliaments and governments to

continue exploring the revolutionary potential of the technology in a modern context and its influence on the future of democracy.

## References


Belcher, M & Lopes CA 2017, 'Maji Voice Kenya: Better Complaint Management at Public Utilities', in T Peixoto & M Sifry (ed.), *Civic Tech in the Global South: Assessing Technology for the Public Good,* World Bank, Washington, DC.

Bjanarson 2017, *Over half of Reykjavik residents steer policymaking – here's how,* apolitical, 28 September, viewed 20 September 2019, https://apolitical.co/solution_article/half-reykjavik-residents-steer-policymaking-heres/

Chin, C 2016, *Japan Trials AI for Parliament Use,* GovInsider, viewed 30 August 2019, https://www.themandarin.com.au/105012-an-innovative-step-toward-truly-empowered-citizen-governance/

Conley, HA & Vilmer, JJ 2018, *Successfully Countering Russian Electoral Intelligence*, Center for Strategic & International Studies, Washington, D.C.

DeJohn, S 2017, 'Beyond Protest: Examining the Decide Madrid Platform for Public Engagement', *The GovLab,* 13 November, viewed 9 August 2019, http://thegovlab.org/beyond-protest-examining-the-decide-madrid-platform-for-public-engagement/

Department of Finance, Services & Innovation 2019, *NSW Cyber Security Policy,* DOFSI, viewed 9 August 2019, https://arp.nsw.gov.au/dfsi-2019-02-nsw-cyber-security-policy

Doche, C, McCombie, S & Rabehaja, T 2019, *Cyber Attack on the Australian Parliament and the Lessons Learned,* Australian Institute of International Affairs, viewed 9 August 2019, https://www.internationalaffairs.org.au/australianoutlook/cyber-attack-australian-parliament-lessons-learned/

Field, A 2016, 'Why There Isn't More Of A Hullabaloo About Civic Tech', *Forbes,* 11 June, viewed 30 August 2019, https://www.forbes.com/.

Garrigues, J 2017, *How is the Civic Innovation Network Helping Shape the City of Brussels?,* CitizenLab, 25 January, viewed 30 August 2019, https://www.citizenlab.co/blog/news/civic-innovation-network-is-shaping-the-future-of-the-city-of-brussels/

Gass, N 2016, 'FBI Probing DNC Hack', *Politico,* 25 July, viewed 9 August 2019, https://www.politico.com/.

Hartcher, P 2019, 'Farewell tech utopia: how governments are readying the web for war', *The Sydney Morning Herald,* 19 February, viewed 20 September 2019, https://www.smh.com.au/.

Hartley, K 2019, *Unlocking the Potential of Civic Technology,* The Chicago Council on Global Affairs, viewed 20 September 2019, https://www.thechicagocouncil.org/sites/default/files/report_unlocking-potential-civic-technology_20190508.pdf

Hendry, J 2019, 'Crypto Defect Found in Swiss E-voting System', *iTnews,* 12 March, viewed 9 August 2019, https://www.itnews.com.au/.

Lackaff, D 2016, 'Better Reykjavik – Open Municipal Policymaking', in E Gordon & P Mihailidis (ed.), *Civic Media: Technology, Design, Practice*, MIT Press, Cambridge, MA.

Marr, B 2019, 'Artificial Intelligence Can Now Write Amazing Content – What Does That Mean For Humans?', *Forbes,* 29 March, viewed 30 August 2019, https://www.forbes.com.

Mehr, H 2017, *Artificial Intelligence for Citizen Services and Government,* Harvard Ash Center for Democratic Governance and Innovation, Cambridge, viewed 30 August 2019, https://ash.harvard.edu/files/ash/files/artificial_intelligence_for_citizen_services.pdf

Nesta n.d., *vTaiwan,* viewed 9 August 2019, https://www.nesta.org.uk/feature/six-pioneers-digital-democracy/vtaiwan/

NSW Electoral Commission 2019, *iVote Online and Telephone Voting,* NSWEC, viewed 9 August 2019, https://www.elections.nsw.gov.au/Voters/Other-voting-options/iVote-online-and-telephone-voting

NSW Electoral Commission 2019, *NSW Electoral Commission iVote and Swiss Post e-voting,* NSWEC, viewed 9 August 2019, https://www.elections.nsw.gov.au/About-us/Media-centre/News-media-releases/NSW-Electoral-Commission-iVote-and-Swiss-Post-e-vo

NSW Government n.d., *My Community Project,* viewed 30 August 2019, https://www.nsw.gov.au/improving-nsw/projects-and-initiatives/my-community-project/

Parliament of Australia 2019, *Democracy and disinformation,* viewed 20 September 2019, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/AECAnnualReport2017-18/Status_report/section?id=committees%2Freportjnt%2F024259%2F27101

Parliament UK 2017, *Statement Regarding Cyber Incident,* viewed 9 August 2019, https://www.parliament.uk/business/news/2017/june/cyber-incident/

Parliament UK 2017, *Update Following Cyber Security Incident,* viewed 9 August 2019, https://www.parliament.uk/mps-lords-and-offices/offices/commons/media-relations-group/news/update-following-cyber-attack/

Pew Research Center 2019, *Many Across the Globe Are Dissatisfied With How Democracy Is Working,* 29 April, viewed 20 September 2019, https://www.pewresearch.org/global/2019/04/29/many-across-the-globe-are-dissatisfied-with-how-democracy-is-working/

Rahvakogu n.d., *About the Estonian People's Assembly in 2013,* viewed 9 August 2019, https://rahvakogu.ee/peoples-assembly-in-2013/

Roberts, JJ 2018, 'Hackers Breach Dozens of Local Government Payment Portals to Steal Credit Card Data', *Fortune,* 18 December, viewed 9 August 2019, https://fortune.com/.

Rumbul 2015, *Who benefits from civic technology?*, mySociety, London, viewed 20 September 2019, https://www.mysociety.org/files/2015/10/demographics-report.pdf

Sanger, DE & Perlroth, N 2016, 'As Democratic Gather, A Russian Subplot Raises Intrigue', *The New York Times,* 24 July, viewed 9 August 2019, https://www.nytimes.com/.

Scytl n.d., *State of Gujarat India: Internet Voting for Municipal Elections,* viewed 9 August 2019, https://www.parliament.uk/documents/speaker/digital-democracy/GUJARATINDIA.pdf

Service NSW n.d., *Annual Report 2017,* viewed 30 August 2019, https://www.service.nsw.gov.au/sites/default/files/Annual%20Report%20FINAL%20-%202016-17.pdf

Service NSW n.d., *Digital Driver Licence,* viewed 20 September 2019, https://www.service.nsw.gov.au/campaign/digital-driver-licence

Swiss Post n.d., *E-voting,* SP, viewed 9 August 2019, https://www.post.ch/en/business-solutions/e-voting

Swiss Post n.d., *E-voting, SP, viewed 9 August 2019, https://www.evoting.ch/en*

Tan 2018, 'Civic Tech Weekly Aug 20: Exporting China's Surveillance State', *govnews,* 20 August, viewed 20 September 2019, https://g0v.news/.

Tovey, J 2019, 'NSW Election: Technical Problems Down Online Voting and Disrupt Pre-Poll Booths', *The Guardian,* 13 March, viewed 9 August 2019, https://www.theguardian.com/au.

UNESCO 2019, *Japan pushing ahead with Society 5.0 to overcome chronic social challenges,* 21 February, viewed 20 September 2019,

https://en.unesco.org/news/japan-pushing-ahead-society-50-overcome-chronic-social-challenges

Verified Voting n.d., *Internet Voting Outside the United States,* VV, viewed 9 August 2019, https://www.verifiedvoting.org/resources/internet-voting/internet-voting-outside-the-united-states/

vTaiwan n.d., *Where do we go as a society?*, viewed 20 September 2019, https://info.vtaiwan.tw/#three

WA Electoral Commission n.d., *iVote*, WAEC, viewed 9 August 2019, https://www.elections.wa.gov.au/ivote

WA Companion Card n.d., *Register for iVote, WACC, viewed* 9 August 2019, http://www.wacompanioncard.org.au/news-events/63-register-for-ivote

Wytze, A, 'Civic Tech Weekly January 3: Meet Russia's Blockchain e-Voting Platform', *g0vnews,* 4 January, viewed 9 August 2019, https://g0v.news/.

Wytze, A, 'Code for Canada's Civic Tech Playbook for Canadian Municipalities', *Medium,* 15 November, viewed 30 August 2019, https://medium.com.