Submission to the inquiry into the future conduct of elections operating in times of emergency

Vanessa Teague
CEO, Thinking Cybersecurity Pty. Ltd.
A/Prof (Adj.), The Australian National University
vanessa@thinkingcybersecurity.com*

November 13, 2020

Summary
In times of emergency, I recommend

- a longer early voting period,
- easier options for delivering "postal" votes without using the post,
- not allowing Internet voting, web-loading pdfs, phone voting or other forms of unverifiable remote voting.

1 Why Internet voting is not the solution

I have spent 15 years researching the security and privacy of Internet voting systems. The more we learn about this problem, the more we understand how difficult it is.

1.1 Integrity and Verifiability

Internet voting systems introduce a risk for both the secret ballot and the integrity of the results. Our recent work on the SwissPost/Scytl system and the NSW iVote system showed than even sophisticated cryptographic proofs of election integrity could be easily faked. (See [HLPT20] for a technical description and [CEL+19] for a nontechnical description of the main issues.) I have written extensively on these issues in prior submissions and will not reiterate all the details here, but emphasise that the serious risk of undetectable fraud remains an unsolved problem, even in relatively well-regulated and transparent democracies such as Switzerland. iVote has had serious security problems in prior runs

*I am on the Board of Advisors of Verified Voting and have engaged in consulting work for the Swiss Federal Chancellery to examine the cryptographic verification of their e-voting system and make recommendations for improving their regulations.

as well [HT15, CEET17]. Analysis of other Internet voting systems shows similar problems [SFD+14, SKW20]—some have been partially addressed; others remain.

1.2 The secret ballot

Like many Australians, I am increasingly concerned about foreign influence (and inappropriate local influence) on Australian elections. The secret ballot was introduced in the 1850s with the specific purpose of helping less-powerful citizens vote as they truly wished, without being afraid of retribution (or hopeful of receiving favours) from more powerful individuals. That basic reasoning hasn't changed. I believe the secret ballot remains critically important to genuine democracy, whether those in need of protection are working-class white males, young people in insecure work, immigrants from authoritarian countries, or anyone else who might be subject to pressure. Voting over the Internet generally makes it easy for a person to prove how they voted.[1] For example, the iVote system's verification app allows voters to use their voting credentials to query the server and ask what vote has been recorded for them. If, rather than verifying for themselves, they share their verification credentials with someone else, then that outside party can use the same mechanism to check how the person voted. This is a much more pernicious method of electoral influence than misinformation or ads, because even a person who does not believe the propaganda can still be pressured into voting in a particular way.

2 Early voting

Early voting—on paper, in a polling place—could be made much easier and more widely available. This seems to have worked very well in the USA.

Postal voting is a last resort for those who cannot vote in person. I don't think it should be encouraged, and I think that early voting is vastly preferable for both integrity and privacy, but for some people postal voting is necessary. Having said that, postal voting could be much less dependent on the postal service. Many US states give voters the option to hand-deliver their paper ballots into a special locked box, for example at the city hall, polling centre or electoral office. These are placed in an envelope like a postal vote, with the voter's name on an outer envelope and the vote inside a second inner envelope. We have seen this work surprisingly well in the USA—I don't know why Australian electoral commissions don't support it. Obviously it is not as secure and private as voting in a supervised polling place, but it is no worse than postal voting, provides more convenient out-of-hours options than a polling place, and removes reliance on the post to return the mail.

[1] Some academic systems do defend against this, but generally at the cost of significant extra complexity for the voter. The Estonian system attempts to ameliorate the problem by allowing people to re-vote on paper, but this introduces challenges for verifying the results.

3 Conclusion

The troubled US election has shown us, if there was ever much doubt, that integrity and evidence are essential properties of elections. A candidate who loses (or fails to win) the contest, and their supporters, are entitled to demand evidence that they deserved to lose. The world is incredibly lucky that years of work, scholarship and activism have improved US electoral processes to the point where—in most places—a convincing evidence trail supports the announced outcome. By 2020 (but not by 2016), most states have switched from mostly-paperless voting machines to machines that build a paper-based evidence trail. Ironically, the pandemic has partially helped, because even in states with questionable pollsite machine designs (such as Georgia), many votes come in on paper. At the time of writing, the Georgia Secretary of State has just announced a plan for a full manual recount the presidential race using paper ballots. In 2016, that would have been impossible (and likewise in Pennsylvania) because there was no voter-verified evidence trail to count. The existence of that evidence trail may save American democracy.

Australians are accustomed to assuming that electoral processes are trustworthy, so our electoral commissions often emphasise convenience, price and speed over integrity and evidence. The AEC runs the Senate digitisation process on untransparent machines without a rigorous audit; the NSW Electoral Commission takes 5% of its votes from the Internet via an easily-manipulated system, and the ACT's EVACS machines do not even attempt to build evidence of an accurate election outcome. There seems to be an assumption that Australia's tradition of trusted electoral processes means that challenges are unlikely and therefore integrity and evidence aren't so important. This reasoning is backwards: Australia has a long history of peaceful, mostly-uncontested elections *because* election results are usually derived from a transparent process supported by a convincing evidence trail. We destroy that at our peril.

References

[CEET17] Chris Culnane, Mark Eldridge, Aleksander Essex, and Vanessa Teague. Trust implications of ddos protection in online elections. In *International Joint Conference on Electronic Voting*, pages 127–145. Springer, 2017.

[CEL+19] Chris Culnane, Aleksander Essex, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. Knights and knaves run elections: Internet voting and undetectable electoral fraud. *IEEE Security & Privacy*, 17(4):62–70, 2019. `https://dial.uclouvain.be/pr/boreal/object/boreal%3A219008/datastream/PDF_01/view`.

[HLPT20] Thomas Haines, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. How not to prove your election outcome. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 644–660. IEEE,

2020. https://dial.uclouvain.be/pr/boreal/object/boreal%3A223906/datastream/PDF_01/view.

[HT15] J Alex Halderman and Vanessa Teague. The new south wales ivote system: Security failures and verification flaws in a live online election. In *International conference on e-voting and identity*, pages 35–53. Springer, 2015.

[SFD+14] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J Alex Halderman. Security analysis of the estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 703–715, 2014.

[SKW20] Michael A Specter, James Koppel, and Daniel Weitzner. The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pages 1535–1553, 2020. https://www.usenix.org/system/files/sec20-specter.pdf.