RESPONSE TO THE QLD GOVERNMENT'S DISCUSSION PAPER ON ELECTORAL REFORM

Vanessa Teague, Research Fellow, University of Melbourne

I have made a number of submissions on electronic voting security, verifiability and transparency to various Australian parliaments. Much of the following text is taken from my submission to the Victorian parliament. Further details on other systems are available as CORE submissions to the NSW, Victorian and federal parliaments. I would be happy to discuss or expand upon these issues, or any issues raised in my other submissions. [redacted]

I am endorsed by the executive of CORE as an Expert for the purposes of this submission. The Computing Research and Education Association of Australasia, CORE, is an association of university departments of computer science in Australia and New Zealand.

I have been working (on a voluntary basis) with the Victorian Electoral Commission on their current project based on prêt à voter.

INTRODUCTION: ELECTRONIC VOTING

Achieving transparency and verifiability in computerised voting is very difficult, because a person cannot observe directly what a computer is actually doing. A voter interacting with a PC, or a group of scrutineers watching a display screen, cannot actually observe what is happening to the electronic data. Hardware and software errors, accidental configuration errors, or deliberate manipulation or hacking, could all cause privacy to be breached or votes to be modified, misrecorded or dropped. A brief look at a week's technical news shows that electronic security breaches on important government and financial infrastructure are common. For example, last week's news included a story on a Chinese hacking group that compromised numerous financial, technological and (US) government targets (BBC, 2013). Electronic voting systems would not be immune.

Transparency, privacy and verifiability have been fundamental requirements of Australian electoral administration since long before computers were involved. Much of the current nationwide debate on voting technology centres on how to adapt these principles to computerised elections. There are two important themes:

*1. **Transparency**, in form of the system's source code and documentation being publicly available for open review.*

*2. **Verifiability**, in the sense that for each election, each voter should get good evidence that their vote is cast in the way that they intended, and scrutineers and the public should get good evidence that all the votes are properly input and accurately tallied.*

Verifiability can be achieved reasonably easily in a supervised polling place, using a human-readable paper printout. This is described next. The following section explains why usable, verifiable remote Internet voting is an unsolved problem in the context of the sort of security threats that are common on the Internet.

ATTENDANCE ELECTRONICALLY ASSISTED VOTING: VARIOUS OPTIONS

The idea of verifiability applies to all elections, not just electronic ones. Unlike elections conducted in a single polling place and based on paper, electronic processes are inherently opaque to observers, so even a group of scrutineers standing around the computer cannot actually verify directly that it is doing the right thing to the ballot data. Nor can a voter using a computer verify directly that the computer is writing the electronic vote that the voter wanted.

"Verifiability" needs to be made precise in order to be meaningful. Indeed, many electronic voting software vendors advertise "verifiable" products which in fact provide very little meaningful evidence of having achieved the correct result.

"Voter verifiability" (sometimes called cast-as-intended verifiability) is the first step – this is where a voter gets evidence that their vote is cast as they intended it. A verifiable election also needs to show that the vote was properly dealt with after that. It should be possible for voters and observers to verify that all the votes were counted as the voter cast them, and then correctly tallied. Systems with all three kinds of verifiability are called "end-to-end" verifiable because every step of the process is verifiable. Prêt à voter is an end-to-end verifiable voting scheme.

Secure, usable, transparent and verifiable electronically-assisted voting in a supervised polling location is a solved problem, and there are various sensible options. Two good examples are:

1. **Computer-assisted attendance voting with a human-readable paper trail.** A computer assists a voter to fill in a vote, which is then printed and placed in a ballot box and treated the same way as all the other votes. This solution is used in Tasmania. It is a simple and voter-verifiable solution. If the voters are a mix of sighted and vision impaired, then many of them can check that the vote is cast in the way that they requested. It provides a degree of verifiability and privacy that is comparable to traditional paper-based attendance voting.
2. An **end-to-end verifiable voting system**, such as the VEC project based on prêt à voter. Each election, voters will get good evidence that their votes are cast in the way that they intended, and properly included in the count, and there will be a public proof that all the votes (from this system) are accurately output. This provides each voter with a mathematical proof that their vote was accurately included in the count.

The choice between options 1 and 2 should depend on exactly what the system will be used for. The crucial advantage of (2) over (1) is that the voters take home a receipt that provides evidence of the correct inclusion of their vote; there is no need to retain a paper trail at the polling place (or transport a paper trail back to a counting centre) because a full electronic proof is provided to everyone. However, the system is more difficult to administer and use than the simpler "Tasmanian" system, which relies instead on a secured trail of paper votes. In either of the above cases, it would be reasonable to extend eligibility to everyone who wanted to use the system, rather than restricting it to just those voters who would require assistance voting on paper.

The ACT open-source system set a high standard for transparency when it was introduced more than a decade ago, but does not provide a human-readable record of the vote for verification.

Recommendation: *For each election, each voter should get good evidence that their vote is cast in the way that they intended, and scrutineers and the public should get good evidence that all the votes are properly input and accurately tallied. If electronic voting is extended to voters who can read their own printout, then it should provide a printout for them to verify (a voter-verifiable paper trail), or some other form of direct verification.*

SECURE INTERNET VOTING: AN UNSOLVED PROBLEM

Secure and usable remote electronic voting, i.e. Internet voting, remains an unsolved problem. There are various software products available that purport to provide security and verifiability, but experience in other states, particularly NSW, has shown serious problems relating to reliability, security and verifiability. This is discussed in our submissions to the NSW parliament (Teague & Wen, 2012). Most computer scientists recommend strongly against returning voted ballots over the Internet at present.

The main outstanding technical challenges are:

1. **Cast-as-intended verifiability**, otherwise known as defence against a compromised client (PC). There is considerable research into end-to-end verifiable cryptographic protocols for remote (Internet) voting, and some academic systems exist, but none of them are ready for deployment in real elections. The main reason is that these protocols demand considerable work and understanding from the voter.
2. **Voter authentication.** Making sure the person casting the vote is the eligible voter you think they are. Voter authentication is a significant challenge in any kind of voting, but the possibility for large-scale fraud increases when remote electronic options are available.
3. **Verifying the votes are counted as cast and tallied correctly.** This is challenging, but techniques do exist and could possibly be adapted from the prêt à voter project.
4. **Privacy** is a serious issue, though it is also a serious issue in postal voting.

For example, the system advertised in NSW as "confirm[ing] there has been no tampering to the vote" (NSWEC, 2011) in fact proved nothing of the kind. Although Internet voting had been widely accepted in Estonia, the party that came second in the most recent election refused to accept the results and challenged the election outcome on the basis of alleged lack of secrecy, security and reliability of Internet voting (OSCE, 2011).

At present no Internet voting solution exists that provides a degree of security and verifiability as good as postal voting for those who can fill in their own postal vote. For voters who need assistance filling in their own paper vote, the two verifiable attendance electronic voting solutions mentioned above provide superior security and verifiability to any Internet voting solution now available, or likely to be available in the near future. Disabled voters' democratic rights are not improved by providing an accessible remote voting solution that does not protect the integrity of their vote as well as alternative methods.

ELECTRONIC DELIVERY AND PAPER RETURNS

I have previously suggested electronic delivery of ballot information and paper (postal) voting returns, especially for local government elections which are otherwise a significant burden on the postal service. Although this remains subject to some of the same vulnerabilities of postal voting, it at least gives voters the opportunity to verify that they send the vote they intended to send. This may help to address some of the problems that seem to need Internet voting.

TRANSPARENCY

Recommendation: *As much as possible of the system's technical details (including source code) and documentation (including documentation on the development processes and reports on the audit and evaluation) must be available to scrutineers, security experts and the public. This level of transparency should be an enforced condition of the initial tender and contract.*

Transparency of electronic voting systems has become quite controversial in Australia, but it's really very simple: the more scrutiny that can be applied to more details of the software system, the more assurance that it does what it's supposed to. Achieving the same standard of transparency as traditional voting methods requires planning and support for openness to counter the inherently non-transparent nature of IT systems. Even then, source code availability should be enhanced by enough support for compiling, running and understanding the system.

Making a system open source does not automatically make it secure---I said this clearly to both the NSW JSCEM and the Victorian EMC. However, keeping its source code secret does not make it secure either. Transparency is good for security, because bugs and vulnerabilities have a better chance of being identified and patched before the election. Having the open source available to the community for technical review by a range of interested experts will increase transparency of the electronic voting process and enable a wide range of expertise to be deployed. The VEC's new project based on prêt a voter will have, and the ACT project based on EVACS already has, openly available source code.

The reason this issue is so contentious is that the business interests of software vendors differ from the transparency requirements of election administration. A vendor's priority is its commercial interest. Its obligations are to protect the value of the IP related to its product and also the value of its reputation (obviously it's bad for business if failures, vulnerabilities and shortcomings come to light).

There is a subtlety about open-source requirements and the degree of trust placed in the system. For example, the Tasmanian-style electronic ballot marker could malfunction and misrecord ballots, but any misrecording or malfunction would be immediately obvious to the voter when they checked their printout.

Hence the argument about the necessity of open source code is less forceful. By contrast, the iVote system (at least in its current form) provides no meaningful verifiability, so it's all the more important for the technical details to be available for review. Queensland will need to decide how much trust is going to be placed in the system, and set transparency requirements accordingly.

CONCLUSION

Enhancing access for voters with disabilities and decreasing accidental informal voting are both important benefits that come from electronically assisted voting. It's important that these benefits come with a continued emphasis on verifiable election outcomes and transparent electoral processes.

In general anything that uses technology for improved communication with voters is probably an improvement. However, technology that is used as a trusted medium for taking and transferring votes needs to be approached with great caution, and subject to the extensive scrutiny and verification applied to other processes that take and transfer votes.

Currently available technology includes several sensible options for electronically assisted voting in a supervised polling place, which allow a voter to verify from a human-readable printout that their vote is cast as they intended, and provide varying degrees of evidence about the correctness of the downstream process. No currently available technology provides adequate security or verifiability for Internet voting.

BIBLIOGRAPHY

BBC. (2013, Feb 19). *China military unit 'behind prolific hacking'.* Retrieved from BBC News: http://www.bbc.co.uk/news/world-asia-china-21502088

NSWEC. (2011). *iVote Approved Procedures for 2011 NSW State General Election.* Retrieved from http://www.elections.nsw.gov.au/publications/policies/ivote_approved_procedures/4._approved_procedures/4.8_authentication_of_vote

OSCE. (2011). *The organisation for security and cooperation in Europe (OSCE) report on the Estonian election.* Retrieved from www.osce.org/odihr/77557

Parliament of New South Wales, Electoral Matters Committee. (2012). *Administration of the 2011 NSW Election and related matters (Final Report).* Sydney.

Teague, V. (2011). *CORE Submission to the Inquiry into the 2010 Victorian State Election.* Retrieved from http://www.parliament.vic.gov.au/images/stories/committees/emc/2010_Election/submissions/13_VTeague_EMC_Inquiry_No.6.pdf

Teague, V., & Wen, R. (2012). *CORE submission to the Inquiry into the administration of the 2011 NSW election.* Retrieved from http://www.parliament.nsw.gov.au/Prod/parlment/committee.nsf/0/BA09355EDE5E3859CA2579AD0001D53C

Teague, V., & Wen, R. (2013). *CORE submission to the inquiry into 2012 local government elections.*