Submission 114
Date Received: 7 March 2014

SUBMISSION TO PARLIAMENT OF AUSTRALIA JSCEM INQUIRY INTO THE 2013 FEDERAL ELECTION

Prof Rajeev Goré
Research School of Computer Science
The Australian National University

Dr Vanessa Teague
Computing and Information Systems,
University of Melbourne

This submission addresses security, privacy, transparency and verifiability of electronic voting and vote counting. We would be happy to discuss or expand upon these issues, or any issues raised in our previous submissions.

Prof Rajeev Goré is the leader of the Logic and Computation Group at ANU. His expertise is in using logic to verifying correctness of programs, including those that count votes. He did some paid consulting work on electronic vote-counting in 2005. He is currently a chief investigator on an Australian Research Council Discovery Grant on verified vote counting. Dr Vanessa Teague is a research fellow at the University of Melbourne. Her expertise is in using cryptography to verify correct treatment of data, particularly voting data. She has been working (on a voluntary basis) with the Victorian Electoral Commission on their current project based on prêt à voter.

Neither author has any financial interest in electronic voting.

We are endorsed by the executive of CORE as experts for the purposes of this submission. The Computing Research and Education Association of Australasia, (www.core.edu.au), is an association of university departments of computer science in Australia and New Zealand.

Contents

SUMMARY OF RECOMMENDATIONS:

Recommendation 1 [Transparency]: *The system's source code and documentation should be publicly available for open review. In particular, we support the request to make the AEC's Senate counting code openly available.*

Recommendation 2 [Verifiability]: *For each election, each voter should get good evidence that his or her vote is cast in the way that he or she intended, and scrutineers and the public should get good evidence that all the votes are properly input and accurately tallied.*

Recommendation 3 [Counting algorithm verification]: *formal verification that the computer code for (STV) vote-counting correctly implements the count is also possible using modern software verification techniques.*

Recommendation 4 [Internet Voting]: *Secure and usable remote electronic voting, i.e. Internet voting, remains an unsolved problem. If Internet voting is introduced, it should be only with the clear public explanation that the privacy and integrity of the system are significantly below those of postal voting. It is a last resort with limited integrity guarantees, appropriate at best for those who do not get high integrity or privacy guarantees with alternative systems. This does not include ordinary postal voters.*

Recommendation 5 [Electronic delivery and paper returns]: *We should consider alternative methods of using the Internet without necessarily trusting it alone to carry completed ballots.*

Recommendation 6 [Cast-as-intended verification]: *secure voting by computer in the polling place is feasible provided it has a human-readable paper trail for sighted voters, or some other form of direct verification.*

INTRODUCTION

The potential advantages of electronic voting are obvious, but the risks are not. Computers could help voters who would otherwise need human assistance, and could protect all voters from accidentally voting informally. However, voters' democratic rights are not enhanced if their votes can be manipulated, their privacy can be violated, or if the system fails to provide evidence that stands up to dispute.

This submission considers three ways of including computers in elections:

1. **Electronic counting of STV votes (p.7),**

   This should be conducted using an open-source counting program, preferably one that has been formally verified to implement the count correctly.

2. **Electronic voting in a supervised polling place (p.11),**

   Voters should get direct evidence from a human-readable paper record that their vote is cast as they intended. That evidence should be linked to a meaningful way for scrutineers or observers to check that the votes are included unaltered in the tally.

3. **Internet voting (p.8).**

   Secure and usable Internet voting suitable for Australian elections is an unsolved problem.

The single most important property of any election, whether it is paper-based or computer-based, is our ability to scrutinise and challenge each and every aspect of the process in a transparent and verifiable way. We trust electoral officials to act honestly, but allow scrutiny by observers when ballots are transported, opened, and counted.

As the debacle in Western Australia has shown, our paper-based elections are not perfect, but they meet the above criterion because the parties involved were able to conclude with confidence that some ballots went missing and that the missing ballots cast enough doubt on the result to make it unacceptable. However, paper-based elections can be slow to produce results, are becoming increasingly logistically difficult and impinge on the privacy of impaired voters who must be assisted by others to cast their vote. The challenge is to use computers while preserving confidence in the election through openness to meaningful scrutiny.

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, dropped or miscounted. Particularly insidious is the fact that all of these could happen without being detected!

Electronic security breaches on important government and financial infrastructure are common. For example, last month an attack on a government website in the US state of Oregon caused "elections and business databases to go offline". The attack was described as "an orchestrated intrusion from a foreign entity" (Zheng, 2014).[1] In 2012 a sophisticated Trojan stole € 36 million from European Internet banking systems (Kalige & Burkey, 2012). Even more concerning are stories of systematic compromise of Internet sites and infrastructure by the Chinese People's Liberation Army (Mandiant, 2013) and the US NSA[2]. Last week it was revealed that half a billion dollars' worth of bitcoins had been stolen from one of the world's largest bitcoin exchanges (Sydney Morning Herald, 2014). Electronic voting systems would not be immune from such attacks. Indeed, Internet voting is harder to secure (for privacy reasons) and has higher stakes than most other Internet applications (Jefferson).

The challenge is to adapt existing principles of transparency, privacy and verifiability to computerised elections. A vital question to ask is this: will the electronic vote-casting and vote-counting system withstand a legal challenge in the Court of Disputed Returns? There are two important themes:

Recommendation 1 [Transparency]: The system's source code and documentation should be publicly available for open review.

Recommendation 2 [Verifiability]: 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.

Paper processes are not perfectly secure or reliable, but neither are computers. For example, the lost vote rate in the 2013 West Australian Senate race (1370 out of 1,348,797, slightly over 0.1%) was about the same as the demonstrated vote misrecording rate in Australia's largest Internet voting trial, the NSW iVote project (43 misrecorded electronic votes out of 46,864, slightly under 0.1%) (PWC, 2011). The WA Senate incident received much more attention because it impacted an election outcome, not because the system was inherently much less reliable. Even more importantly, the paper-based Senate process retained paper evidence of the 99.9% of votes that weren't lost; the iVote system produced

[1] This website was not used for Internet voting, but for databases related to issues such as campaign finance.

[2] Schneier: "The NSA also attacks network devices directly: routers, switches, firewalls, etc. Most of these devices have surveillance capabilities already built in; the trick is to surreptitiously turn them on… "; Snowden: "Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."

no meaningful evidence of the correctness of any of the votes. Reliability, privacy and verifiability must be designed into electronic voting processes as carefully as they are designed into our existing paper-based processes.

In a polling place, many sensible solutions are available, all involving a human-readable paper record so voters can check that their vote is cast as they intended. Some alternatives and tradeoffs are discussed from p. 11. There are no sufficiently secure, private and verifiable options for Internet voting. This is explained from p. 8. This submission examines both these alternatives with an emphasis on the transparency, verifiability, privacy and security of the possible solutions.

We begin with a discussion of transparency in the form of source code availability. This is particularly relevant for electronic (STV) vote counting, but applies to all other aspects of electronic voting too.

TRANSPARENCY

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 is supposed to do. It is harder to run a transparent electronic process than a transparent paper one, because software is harder to understand and follow than familiar manual procedures.

Computerised voting systems, including their source code, all documentation and reports, and the associated physical security procedures should be available to e-voting and security experts and the public. Source code availability should be enhanced by enough support for compiling, running and understanding the system. This level of transparency should be an enforced condition of the initial tender and contract.

Making a system's source code public does not automatically make it secure or correct. However, neither does keeping its source code secret. Transparency is good for security, because bugs and security 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 and trustworthiness of the electronic voting and counting process, because it facilitates an open and scientifically informed discussion about the merits of a proposed system. It also helps find bugs.

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).

Internationally, some countries (such as Switzerland) continue to use closed-source Internet voting systems. Others, such as Norway, have been open-source all along, while others, such as Estonia, have made their systems open following public pressure[3].

"Auditing" or "certification" by third parties is not a substitute for electoral transparency. Auditing firms do not have the same incentives as candidate-appointed scrutineers. The history of electronic voting "certification" and "auditing", both in Australia and overseas, has produced "certification" reports for systems that actually had serious security vulnerabilities or software errors, including the NSWEC iVote system (PWC, 2011), the VEC 2007 Scytl system[4] (Teague, 2011), (Scytl Secure Electronic Voting, 2011), and the systems by Diebold, Hart and Sequoia analysed in the California Top to Bottom Review. The NSW and Californian examples are discussed more below.

STV COUNTING

Australian elections invariably use some form of preferential voting where voters are asked to order a list of candidates by numbering the candidates in order of the voter's preference. Counting such ballots by hand is a notoriously difficult task, especially for STV. Consequently, more and more electoral commissions are turning to computers to count the ballots, whether they be cast electronically or via paper. This raises the question of whether the computer program that counts the ballots does so correctly. As demonstrated by the WA election, tens of votes out of millions can make a difference to the end result. Thus interested parties are highly likely to challenge a result that is close.

For example, the Logic and Computation Group at the ANU have found three bugs in the vote-counting module of EVACS, the ACT's open-source electronic voting and counting system. All have been acknowledged by the ACTEC (Elections ACT). Two of them were found by scrutinising the code, but a third was found by running a counting program developed independently by ANU researchers, and tracing the differences in the scrutiny sheets produced by the official program and this ANU program (Dawson, Goré, & Slater, 2003). Each of these bugs could have changed the outcome of the election. Fortunately, none of them manifested themselves in the five elections that have used EVACS: 2001, 2002, 2004, 2008 and 2013. This illustrates several points:

1. ``quality certification'' is meaningless because the code had been "audited" by a commercial quality assurance company, BMM Australia;
2. serious bugs can lie undetected for years;
3. fixing the bugs does not guarantee anything since there may well be other bugs.

[3] The Estonian source code is available at https://github.com/vvk-ehk/evalimine
[4] The most serious issue, identified by V Teague, was patched before the election.

We believe the Australian Electoral Commission would benefit greatly in the long term from making its STV counting source code publicly available, as requested under the Freedom of Information Act last year (Cordover, 2013). Although the (probable) discovery of some errors might be temporarily embarrassing, in the long term transparency improves the chances of announcing a correct and defensible Senate outcome.

The Victorian Electoral Commission and ACT Electoral Commission have both made their STV counting source code open[5]. It is interesting to note that several independent implementations of federal Senate counting exist (for instance, one by Antony Green and one described at http://blog.angrygoats.net/2014/01/25/counting-the-west-australian-senate-election/). These allow independent parties to redo the Senate count. So far they have found no discrepancies, but that is no guarantee that either their code or the AEC's is correct.

FORMALLY VERIFIED VOTE-COUNTING PROGRAMS

Recommendation 3 [Counting algorithm verification]: *formal verification that the computer code for vote-counting correctly implements the count is also possible using modern software verification techniques.*

Modern software verification techniques are now capable of formally verifying that a moderately large computer program does what it is supposed to do. Thus it is perfectly feasible to formally verify that the vote-counting program does indeed count the votes correctly according to the intended STV method.

Of course, none of this obviates the need for scrutineers to be able to check that the paper votes cast by voters match the electronic records entered into the STV count. If they are cast on paper, this is a simple matter of returning to the paper records. If they are cast on a computer, this raises a whole new set of questions about how to verify that the voter's intentions are accurately captured.

(REMOTE) INTERNET VOTING

The rest of this submission details the verifiability of various options for remote and in-person electronic voting. Everything already said about electronic counting applies here as well, but from now on we focus on evidence that the votes are recorded as the voter intended, transferred securely, and accurately reported.

Secure and usable remote electronic voting, *i.e.* Internet voting, remains an unsolved problem. There are various software products available that claim to provide security and verifiability, but experience in other states, particularly NSW, has shown serious problems

[5] The VEC's is at https://www.vec.vic.gov.au/Vote/vote-VEC-ems.html, under "Computerised vote counting"; the ACTEC's at http://www.elections.act.gov.au/__data/assets/file/0004/8185/evacs2012.zip

relating to reliability, security and verifiability. This is discussed in CORE's submissions to the NSW JSCEM (Teague & Wen, 2012). Most computer scientists recommend strongly against returning voted ballots over the Internet at present.

Recommendation 4 [Internet Voting]: Secure and usable remote electronic voting, i.e. Internet voting, remains an unsolved problem. If Internet voting is introduced, it should be only with the clear public explanation that the privacy and integrity of the system are significantly below those of postal voting. It is a last resort with limited integrity guarantees, appropriate at best for those who do not get high integrity or privacy guarantees with alternative systems. This does not include ordinary postal voters.

The main outstanding technical challenges are:

1. **Cast-as-intended (voter) verifiability**, otherwise known as defence against a compromised client (PC). This means giving each voter evidence that their (electronic) vote matches their intention, and has not been manipulated or misrecorded.

2. **Voter authentication**. This means ensuring that the person casting the vote is the eligible voter they claim to be. 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 reported or tallied correctly.** This means producing an electronic analogue of the scrutineered paper-handling or paper-counting process in which observers watch the ballot boxes all day, including as they are opened and their contents counted. Some electronic systems produce a paper record for manual counting; others input the electronic vote directly into an electronic count. Either way, they need to prove that the (paper or electronic) vote record matches what the voter cast.

   If the votes are counted electronically, ensuring that the tallying program is itself correct is a major unresolved issue, as described above.

4. **Privacy** is a serious issue, though it is also a serious issue in postal voting. This includes both physical observation of the person voting, and electronic observation of the vote they have cast.

There is considerable research into end-to-end verifiable cryptographic protocols for remote (Internet) voting, mainly addressing the two types of verifiability mentioned as (1) and (3). For example, the Helios voting system (https://vote.heliosvoting.org/) is an open-source implementation of an Internet voting system that includes both cast-as-intended (voter) verifiability and a full mathematical proof that all the votes are counted as cast and tallied

correctly. Helios can prove correctness for simple counting algorithms, but would be difficult to extend to preferential elections. At the time of writing no fully verifiable Internet voting system is ready for deployment in real elections. The main reason is that these protocols are very complex and demand considerable work and understanding from voters, scrutineers and election officials. Furthermore, they do not address issues associated with voter authentication, or all issues associated with privacy or coercion.

Many available software products claim to be verifiable but aren't. For example, the system advertised in NSW as "confirm[ing] there has been no tampering to the vote" (NSW Electoral Commission) in fact proved nothing of the kind. Although Internet voting had been widely accepted in Estonia, the party that came second in the 2011 parliamentary elections complained to the Estonian Supreme Court, requesting cancellation of the election result on the basis of alleged lack of secrecy, security and reliability of Internet voting (OSCE/ODIHR, 2011). Both Internet voting protocols are being modified in an attempt to address these issues.

Even very simple kinds of fraud could be successfully perpetrated against an Internet voting system. For example, some US political candidates have set up websites apparently soliciting donations for their opponents, but actually keeping the money for their own campaign (Wadhwa, 2014). Similar attacks based on phishing for Internet banking accounts appear in an average inbox almost daily. It would be very difficult to defend an Internet voting application against this sort of simple fraudulent misdirection. Likewise against ordinary distributed denial of service (DDoS) attacks, such as that deployed against an Internet voting system in Canada (Elections BC, 2014).

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 paper vote, the verifiable polling-place electronic voting solutions described below 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.

VOTING BY EMAIL (NOT RECOMMENDED)

Voting by email is a particularly insecure form of Internet voting. Although commonly (correctly) understood to present serious problems for privacy, email voting also presents a serious risk to integrity. Email accounts are hacked all the time, and email contents or attachments can be modified at the sender's end, the receivers end, or in many cases in transit.

ELECTRONIC DELIVERY AND PAPER RETURNS (RECOMMENDED)

Teague has 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. The idea would be that voters access their list of candidate and party names online, fill out their ballot at home, and then mail it in. Although this remains subject to some of the same vulnerabilities as postal voting, it at least gives voters the opportunity to verify that they send the vote they intended to send.

In Los Angeles County, voters who have obtained a postal ballot and filled it in at home often come to a polling place and cast it (in a postal-voting envelope) into a special box. This gives them most of the convenience of voting from home and most of the integrity guarantees of voting in a polling place, without any need to queue. This could be combined with electronic delivery of ballot information, and might improve convenience for some postal voters in Australia.

Recommendation 5 [Electronic delivery and paper returns]: We should consider alternative methods of using the Internet without necessarily trusting it alone to carry completed ballots.

POLLING-PLACE ELECTRONIC VOTING

Are computers secure as long as they are disconnected from the Internet? The simple answer is no. Although the opportunities for remote attack are reduced, significant opportunities for privacy invasion and vote manipulation could remain. Fortunately, elections conducted in a supervised polling place can be verifiable and reasonably private, while taking advantage of the assistance of computers. Voters should have the opportunity to verify a human-readable paper record of their vote, then the rest of the process should let scrutineers (or the voters themselves) verify that all votes are correctly transported and reported.

Recommendation 6 [cast-as-intended verification]: secure voting by computer in the polling place is feasible provided it has a human-readable paper trail for sighted voters, or some other form of direct verification.

It is not enough to test the software or hardware before the election. The system should be designed to provide direct evidence of a correct election outcome.

SECURITY ISSUES THAT REMAIN, EVEN WHEN THE COMPUTER IS DISCONNECTED FROM THE INTERNET

When computerised elections became common in the US after 2000, they were often standalone machines, disconnected from the Internet. Many produced all-electronic election records without a paper backup. Concerns from US computer scientists motivated

the authorities in California to conduct a "top-to-bottom" review in 2007 of the security of the main brands of machines that had until then been used in California (California Secretary of State, 2007). The analysis team successfully compromised all of the machines they studied, in ways that could have led to undetectable electoral manipulation if they had been perpetrated in a real election. One team wrote:

"The testers discovered numerous ways to overwrite the firmware of the Sequoia Edge system, ..., the attackers controlled the machine, and could manipulate the results of the election."

These insecure systems had already been "certified" by an "independent" testing lab. However, in the light of the Top-to-bottom review, they were decertified. Californian legislation now requires all electronic voting machines to produce a voter-verifiable paper record for auditing or manual counting.

Polling place electronic voting machines were purchased for Ireland and then never used, after security researchers demonstrated serious privacy and integrity flaws. The total cost of buying, storing and scrapping the machines was more than €50 million.

Although the ACT's EVACS voting system set a laudable standard for transparency when (at least some parts of) its source code was made available, its design does not adequately defend against attacks on the machines themselves. Indeed it seems to have been designed with the assumption that it does not need to address security problems because it is not connected to the Internet. However, many people have significant access to the machines before and during the voting period, so the same kinds of attacks identified in the California top to bottom review could quite possibly apply. Attacks on the firmware or BIOS could remain undetected even when the computer is supposed to boot from another source (Butterworth, 2013).

The following section describes two methods of providing verifiable election outcomes. Both use a human-readable vote printout.

VERIFIABLE POLLING-PLACE ELECTRONIC VOTING

Computer-assisted voting in a polling place is a solved problem with several sensible solutions. They all involve a human-readable paper record, which the voter can check to see that their vote is cast as they intended.

"Verifiability" needs to be made precise in order to be meaningful. Many electronic voting software vendors advertise "verifiable" products which in fact provide very little meaningful evidence of having achieved the correct result. Some examples of genuinely verifiable solutions are given below:

- **Computer-assisted attendance voting with a human-readable paper trail.** The voter interacts with a computer, which then prints out their vote for insertion into an ordinary ballot box alongside all the other votes. This allows each voter to verify that the printout matches their intentions. Then scrutineers observe the counting process just as they observe all the other paper ballots being counted. This simple and voter-verifiable solution is offered in Tasmania and WA to voters who have difficulty using paper and pencil.

  Several other election authorities, particularly in the USA, use a combination of electronic assistance and a voter-verifiable paper record. Variants include optically scanned paper ballots, electronic voting with a voter-verifiable paper audit trail (VVPAT), and a few others. The unifying theme is that the voter can see a permanent paper record of their vote, which is retained as evidence.

- **The VEC's end-to-end verifiable attendance voting project, based on prêt à voter.** This system uses complex cryptography to provide each voter with good evidence that their votes are cast in the way that they intended, and included unmodified in the count, and a public mathematical proof that all the votes (from this system) are accurately output. Voters verify a printout of their vote, and then take home a receipt, which does not prove how they voted, but can be used later to check that their vote has been included without modification. V Teague has been working on a voluntary basis on this system.

The crucial advantage of prêt à voter over the "Tasmanian" system above is that 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. Hence it is particularly well suited to early and absent attendance voting. 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. It remains to be seen whether the increased complexity of this system is tolerable for voters, scrutineers or electoral officials. In either of those two 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.

TRANSPARENCY AND VERIFIABILITY OF SOME EXAMPLE INTERNET VOTING SYSTEMS

The NSW iVote Internet voting project.

The NSW iVote system, provided by Everyone Counts, gave voters a receipt number which was advertised as "confirm[ing] there has been no tampering to the vote". In fact tampering at the voter's PC or the electoral commission's server (before the receipt number was computed) would not have been detected by this mechanism. Hence the system had no meaningful verifiability.

A new version is proposed that would allow voters to "verify" their vote with an auditing firm after casting it via the New South Wales electoral commission server. Voters will contact the auditor (using their ID number) to check the vote that the electoral commission has recorded for them, then the auditor will promise to make sure that goes into the count accurately. This raises serious concerns for privacy. More importantly, it provides only the auditor's attestation of integrity, which is far short of the traditional demonstration of evidence before scrutineers.

Norway

Norway runs an Internet voting scheme based on sending "confirmation codes" by conventional mail, and later sending a matching code to the voter's mobile phone to confirm their vote. The Norwegian authorities insisted on open source code from the inception of the project. Both the protocol and the source code have been analysed extensively by Norwegian and foreign researchers. The protocol includes defences against some of the attacks mentioned above, but does not provide full end-to-end verifiability.

The Norwegian authorities do not have a genuinely and fully verifiable voting system (despite more optimistic claims from the software vendor), but they have a wealth of technically informed analysis on which to base their decisions.

SUMMARY AND CONCLUSION

The most secure way to vote is in a supervised polling place. A computer in a polling place can help prevent accidental informal voting, and help voters with disabilities to vote independently. However, the system must provide a human-readable paper record so that the voter can check that their vote is cast as they intended (Recommendation 6). This record should be linked to a method allowing scrutineers or voters to check that the record is included unaltered in the count (Recommendation 2).

There are few good solutions for remote voters, and no good solutions for returning voted ballots over the internet (Recommendation 4). It is worth considering sending out blank ballots via the internet and returning a filled-in paper ballot (Recommendation 5).

For either kind of system, the system's source code and documents should be openly available (Recommendation 1). For electronic STV counting especially, the software could benefit greatly from formal verification of its correctness if made publicly available (Rec 3).

If a polling-place electronic voting system provides direct verification that the voter's vote was captured as intended as outlined in Recommendation 6, and evidence of correct inclusion (Recommendation 2), and if the STV votes are counted correctly with an open-source formally verified vote-counting program (Recommendations 1 and 3), then it is very difficult to argue against their result in a court of disputed returns.

SOME COMMENTS ON THE NATIONAL DEBATE

Policymakers and election officials need an accurate understanding of the technical facts in order to make good decisions. Many software products that purport to increase participation or improve privacy for disadvantaged or overseas voters do no such thing, or do so only at the expense of the integrity of the vote. An accurate technical assessment of the proposed solution, its security, privacy and verifiability, should inform decisions about whether and how widely it should be deployed.

A major reason for insisting on transparency of source code and other technical details is to allow an informed public debate based on demonstrable facts.

The Electoral Council of Australia and New Zealand recently published a discussion paper on "Internet voting in Australian Election Systems" (Electoral Council of Australia and New Zealand, 2013). In many ways this is a very thoughtful analysis of the possible uses and justifications of Internet voting. However, it notably excludes technical considerations:

"7.8 As noted in Part 1, the extent to which it can be guaranteed that votes cast on the internet will not be susceptible to interference of one form or another has been a matter of vigorous dispute. This paper takes no stand on that issue,..."

It is important to emphasise that this is not a political or social question, but a technical one amenable to rational scientific analysis. A particular software system operating in a particular environment has a certain set of vulnerabilities and errors, which can be analysed if its details are available. It is telling that the dispute has been most "vigorous" for unverifiable systems whose source code and system details remain secret.

(From the ECA report again:) "7.17 The need for new transparency mechanisms to replace those associated with the paper ballot remains a matter of fundamental importance, and one which will rise in significance in direct proportion to the number of people actually using internet voting. Elaboration of such mechanisms is beyond the scope of this paper."

Again we agree, and emphasise that elaboration of such mechanisms for Internet voting is an unsolved problem.

The ultimate test of the verifiability of an electronic voting solution is whether a candidate who disputes an election outcome based on a software system can convince the Court of Disputed Returns that the evidence supporting that system's output is inadequate. A transparent system that provides voters with direct evidence that their votes are cast as they intended, and provides voters or at least scrutineers, with genuine evidence that all the votes are correctly dealt with, is much more likely to stand up to dispute.

BIBLIOGRAPHY

Butterworth, J. (2013). Bios chronomancy: Fixing the core root of trust for measurement.

Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM.

California Secretary of State. (2007). *California top to bottom review of voting*. Retrieved from http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm

Cordover, M. (2013, Oct). *righttoknow.org*. Retrieved from https://www.righttoknow.org.au/request/software_by_which_senate_counts

Dawson, J., Goré, R., & Slater, A. (2003). *Formal Methods Applied to Electronic Voting Systems*. Retrieved from http://users.cecs.anu.edu.au/~rpg/EVoting/

Elections BC. (2014). *Recommendations report to the legislative assembly of British Columbia.* Retrieved from http://www.internetvotingpanel.ca/docs/recommendations-report.pdf

Electoral Council of Australia and New Zealand. (2013). Internet voting in Australian election systems. Retrieved from http://www.eca.gov.au/research/files/internet-voting-australian-election-systems.pdf

Estonian National Electoral Committee. (n.d.). Retrieved from http://www.vvk.ee/voting-methods-in-estonia/engindex/

Jefferson, D. (n.d.). Retrieved from VerifiedVoting.org: https://www.verifiedvoting.org/resources/internet-voting/vote-online/

Kalige, E., & Burkey, D. (2012). *A Case Study of Eurograbber: How 36 million euros was stolen via malware.* Retrieved from http://www.cs.stevens.edu/~spock/Eurograbber_White_Paper.pdf

Mandiant. (2013). *APT1: Exposing one of China's Cyber Espionage Units.* Retrieved from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

NSW Electoral Commission. (n.d.). *iVote Approved Procedures for 2011 NSW State General Election, 4.8.2(3)*. Retrieved from https://www.elections.nsw.gov.au/publications/policies/ivote_approved_procedures/4._approved_procedures/4.8_authentication_of_vote

OSCE/ODIHR. (2011). *Estonia Parliamentary elections OSCE/ODIHR election assessment mission report.* Organisation for security and cooperation in Europe, Office for Democratic institutions and human rights. Retrieved from http://www.osce.org/odihr/77557

PWC. (2011). *iVote Post-implementation report.* NSW Electoral Commission. Retrieved from http://www.elections.nsw.gov.au/__data/assets/pdf_file/0007/93481/iVote_Audit_report_PIR_Final.pdf

Scytl Secure Electronic Voting. (2011). *Comments from Scytl on the CORE report from the electronic voting solution used in the 2010 Victorian Election.* Retrieved from http://www.parliament.vic.gov.au/images/stories/committees/emc/2010_Election/submissions/14_Scytl_EMC_Inquiry_No.6.pdf

Sydney Morning Herald. (2014, Mar 1). Retrieved from

http://www.smh.com.au/technology/technology-news/bitcoin-giant-mt-gox-files-for-bankruptcy-after-537-million-lost-to-hacking-20140303-33ukj.html

Teague, V. (2011). *CORE Submission to the Victorian Parliamentary Inquiry into the conduct of 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, Feb). *CORE Submission to the inquiry into the administration of the 2011 NSW State Election.* Retrieved from http://www.parliament.nsw.gov.au/prod/parlment/committee.nsf/0/ba09355ede5e3859ca2579ad0001d53c/$FILE/Submission%207%20-%20Core.pdf

Wadhwa, T. (2014, Jul 2). *Republicans Using Fake Websites To Trick Donors Is Just The Start*. Retrieved from Forbes.com: http://www.forbes.com/sites/tarunwadhwa/2014/02/07/republicans-using-fake-websites-to-trick-donors-and-the-troubling-ethics-of-online-political-campaigns/

Zheng, Y. (2014, Feb 13). *The Oregonian.* Retrieved from http://www.oregonlive.com/politics/index.ssf/2014/02/frustrations_mount_as_oregon_s.html