Submission to the Inquiry into the 2007 Federal Election

Fraud in Electronic Elections

Roland Wen
School of Computer Science and Engineering
The University of New South Wales

16 July 2008

1 Introduction

The trend towards electronic elections in Australia raises concerns about the increased threat of electoral fraud. Although traditional paper elections are potentially vulnerable to a range of cunning fraud techniques, electronic elections provide numerous and serious additional potential for electoral fraud. In this submission we discuss one such well-known attack to which electronic elections in Australia are currently vulnerable, the *Italian attack*. This a powerful method for bribing and coercing voters in preferential elections. Indeed the discovery of the use of this fraud contributed to radical electoral reform in Italy during the early 1990s, including the eventual abandonment of preferential voting altogether [Cos07].

Electronic counting (recently introduced for counting below the line Senate ballots) is highly susceptible to the Italian attack, and electronic voting (trialled in the 2007 Federal Election) further exposes voters to this type of fraud. Any person or organisation who obtains the voting data (now publicly available in electronic form for a number of elections) would currently be able to perform the Italian attack with little difficulty. For example a husband could check how his wife voted, a minister could check how his congregation voted, and unions could check how their members voted.

Electronic elections have considerable benefits. However the Italian attack is a striking reminder that we need to proceed cautiously and carefully investigate how we adopt new technology. It is important to note that while our submission focuses specifically on the Italian attack, the issues we raise apply more broadly to other types of electoral fraud and the general integrity of electronic elections in Australia.

2 The Italian Attack

The Italian attack, described in detail by Di Cosmo [Cos07], enabled candidates (many of whom had Mafia connections) to force voters to cast specified votes that could later be uniquely identified with each voter. This ability to determine how a voter had actually voted made intimidation possible. Although the secret ballot ensured that ballots remained concealed during the *voting*, the problem arose when the ballots were revealed during the *counting*.

To carry out the Italian attack, a nefarious candidate provided each voter with a unique, carefully-chosen ordering of preferences to cast as the vote. This vote also served as a unique voter ID number. During the counting, corrupt observers noted the particular sequence of preferences in every ballot to create a list of all the votes cast. Afterwards the candidate checked the specified votes against the list of all votes cast. If a specified vote was not in this list, then the corresponding voter had failed to vote as instructed.

The potency of the Italian attack is due to an inherent property of preferential electoral systems: a voter who is given a specified vote cannot cast a genuine vote and rely on the chance that some other voter (who has not been coerced) happens to cast a vote with the same particular sequence of preferences. Hypothetically coerced NSW voters in the

2007 Federal Election for the Senate had better odds of simultaneously winning *every* lottery in the world than of escaping detection by a coercer.

Votes that double as unique voter IDs pose a dilemma: the information needed to count the votes and verify the result is sufficient to commit electoral fraud. The thorough manual scrutiny process in past Australian elections means it is possible that the Italian attack has already occurred here. We are currently examining past election data to find evidence of whether this fraud has been carried out previously in Australia.

With manual counting it is somewhat onerous, but still feasible, to organise the Italian attack on a large scale. With electronic counting, however, it becomes a trivial task.

2.1 The Vulnerability of Electronic Counting

In electronic counting, electoral officials enter the preferences in each ballot into an electronic database. Access to this voting data simplifies the Italian attack because it is trivial to search the database for specified votes. Our concern is that systematic, widespread fraud now becomes a viable risk.

The Victorian Civil and Administrative Tribunal ruled that the electronic voting data is required to be made publicly available under freedom of information legislation [VCA00]. Although this ruling was in the context of Victorian legislation, it appears to be equally applicable to the Commonwealth and other states. Accordingly the Australian Electoral Commission publishes all below the line Senate voting data on its website [AEC07]. Consequently any member of the public could have identified voters using the Italian attack in the last election.

The Commonwealth Electoral Act 1918, s. 323, covers all possible violations of voter anonymity by prohibiting the release of any information "that is likely to enable the identification of the elector". But with subtle fraud techniques such as the Italian attack, it is perhaps not immediately obvious that preference data is such information. Either the Act, supporting regulations, and/or policy should be tightened to ensure this information is not made publicly available in the future.

Even if the electronic voting data is not publicly released, section 273A(6)(a) of the Act provides scrutineers with access to this data. As with any electronic document, it is then difficult to prevent the deliberate or accidental distribution of the voting data to a wider audience.

Suppressing the electronic voting data altogether is the most effective way to mitigate large-scale bribery and coercion through the Italian attack. However this limits the verifiability of the election result. Emerging research in this area, such as our work on anonymous, verifiable electronic counting [WB08], could lead to viable systems that ensure both secrecy and verifiability in the counting. But there is an urgent need for an acceptable short-term solution.

2.2 The Vulnerability of Electronic Voting

In addition to the Italian attack outlined above, there are numerous other well-known vulnerabilities in electronic voting systems, and it is likely there are further as yet undis-

covered classes of problems. The example of the Diebold voting machines in the USA shows how easy it can be to rig electronic voting systems that have been inadequately analysed [FHF06].

Although the AEC has published several reports on the Electronically Assisted Voting Trial and the Remote Electronic Voting Trial systems used in the 2007 Federal Election, insufficient detail has been revealed on the design and implementation of the systems to perform a thorough security analysis. Nevertheless there are clear indications that at the very least these systems lack appropriate protection against the Italian attack.

The trial systems are incompatible with provisions of the Commonwealth Electoral Act 1918 drawn up specifically for the trials. Sections 202AD(1) and 202AK(2) of the Act both stipulate that the systems must provide a printed vote record for each voter, and this record "must not contain any means of identifying the person who cast the vote". But as outlined with the Italian attack, under the systems used in the trials it is possible to identify who cast the vote.

Our concern is that the trial systems were subject to inadequate analysis and review. In particular the auditor's reports contain alarming factual errors and oversights. These reports failed to identify the above problem with voter identification and in fact drew incorrect conclusions. In assessing the security risks, the auditor's report for the remote electronic voting system [BMM07a], s. 10.1(S8), claimed that the "vote data does not associate the voter with the votes". Similarly the auditor's report for the electronic voting machines [BMM07b], s. 8.1(S12), found the machines "do not record any information that identifies a voter". Overlooking the well-known problem of the Italian attack in electronic elections is indicative of the wider lack of analysis and detail in the auditor's reports. This undermines the credibility of the auditor's reports and the confidence in the security and overall integrity of the trial systems.

Developing and evaluating any secure electronic system is a difficult but vitally important task. Even with considerable time, resources and expertise, it is impossible to completely eliminate all errors, and new examples of software failure and security breaches come to light almost every day. To minimise the risk of serious flaws, there must be ample opportunity for thorough analysis by multiple, independent groups before electronic systems are used in live elections.

3 Recommendations

The Committee should:

1. Review the policies and procedures for vote counting and verifying the election result, taking into consideration the Italian attack and other well-known vulnerabilities in electronic election systems.

2. Establish and improve procedures that ensure thorough and open consultation and evaluation of all proposed electronic election systems.

3. Review the policy on audits to ensure that future audits are conducted with appropriate depth, expertise and diligence.

4 Conclusion

Electronic elections certainly have considerable advantages, and there has been a positive response from participants in the electronic voting trials. But there must be more discussion about the trade-offs between the benefits and the risks. If Australia moves to adopt this new technology, we must exercise great care and caution to limit the risk of electoral fraud and avoid compromising the integrity of our elections.

To this end, transparency of the election process plays a key role. We are fortunate that authorities in Australia recognise the need to promote openness. For example the ACT Electoral Commission publishes the source code for part of its counting software. Researchers at the Australian National University subsequently discovered a minor error in the software, and this was corrected by the vendor. But given the complexity of electronic systems, an even greater level of transparency is necessary. Testing and analysing the software alone is still not enough to detect vulnerabilities, such as the Italian attack, that expose intrinsic design weaknesses. Open access to detailed technical documentation on the complete system design is equally important.

Transparency has traditionally centred on the physical conduct of paper elections. Now it must also encompass the complex electronic election systems and how they operate. In exposing the dangers of revealing certain election data, the Italian attack highlights shortcomings of the current approach to elections, especially in the context of electronic elections. Our immediate challenge is to develop thorough and transparent procedures for elections in this new environment.

References

[AEC07] Australian Electoral Commission. *Virtual Tally Room - Senate Downloads*, 2007.
`http://results.aec.gov.au/13745/Website/SenateDownloadsMenu-13745-csv.htm`.

[BMM07a] BMM Australia. *Audit and Certification of a Remote Electronic Voting System for Overseas Australian Defence Force Personnel*, 2007.
`http://www.aec.gov.au/pdf/voting/evoting_reports/adf/aec_adf_audit_report.pdf`.

[BMM07b] BMM Australia. *Audit of AEC's Electronic Voting Machine for Blind and Vision Impaired Voters*, 2007.
`http://www.aec.gov.au/pdf/voting/evoting_reports/bvi/bvi_audit_report.pdf`.

[Cos07] Roberto Di Cosmo. On privacy and anonymity in electronic and non electronic voting: the ballot-as-signature attack.
`http://www.pps.jussieu.fr/~dicosmo/E-Vote/`, 2007.

[FHF06] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Security Analysis of the Diebold AccuVote-TS Voting Machine. http://itpolicy.princeton.edu/voting/, 2006.

[VCA00] Victorian Civil and Administrative Tribunal. *van der Craats v Melbourne City Council [2000] VCAT 447*, 29 January 2000. http://www.austlii.edu.au/au/cases/vic/VCAT/2000/447.html.

[WB08] Roland Wen and Richard Buckland. Mix and Test Counting in Preferential Electoral Systems. Technical Report UNSW-CSE-TR-0809, School of Computer Science and Engineering, The University of New South Wales, Sydney, Australia, 2008. ftp://ftp.cse.unsw.edu.au/pub/doc/papers/UNSW/0809.pdf.