CORE Supplementary Submission to the Inquiry into the 2010 Federal Election

Best Practices for E-election Systems

Roland Wen[1] Vanessa Teague[2] Richard Buckland[1]

[1]
School of Computer Science and Engineering
The University of New South Wales

[2]
Department of Computer Science and Software Engineering
The University of Melbourne

Executive Summary

The widespread adoption of e-election systems (that is, any IT system used for elections) in Australia has introduced many challenges in ensuring the quality and transparency of our elections. So far the development and operation of e-election systems has been in accordance with standard industry practice. However this is inappropriate for mission critical systems where security and reliability are imperative. The current practice has resulted in a number of examples of poor quality e-election systems, which have experienced failures in many recent elections.

In this submission we identify changes that must be made in order to pursue best practices that ensure e-election systems are secure, reliable and transparent. Our submission addresses general issues that are common to all e-election systems including e-voting and e-counting. Additional issues specific to the cryptographic security of e-voting and e-counting have already been addressed in our first submission (CORE, 2011).

The measures needed to raise the standard of e-election systems include the following:

1. rigorous development and auditing processes to ensure the systems meet the highest standard of security and reliability,

2. comprehensive risk assessments involving broad consultation to account for the full range and extent of potential system vulnerabilities and continually evolving threats to election quality, and

3. full transparency of the systems and processes to facilitate oversight and public scrutiny, with particular regard to personal voter information on the electoral roll.

Without doubt achieving best practice for e-election systems is a very difficult and complex task. However we cannot afford further delays given that electoral commissions are in the process of implementing multiple large e-election projects at great expense. Solutions to technical problems can be difficult or impossible to apply to existing e-election systems that are inherently flawed. Moreover some of these issues were previously raised at JSCEM inquiries up to ten years ago, but have yet to be properly addressed. Electoral commissions must be provided with the necessary assistance and resources to promptly deal with these problems, and thereby assure the quality and trustworthiness of e-election systems.

Recommendations

Recommendation 1. *E-election systems must be developed using best practices for mission critical systems rather than standard practices for commercial IT systems.*

1. *The development process must use rigorous, well-established software engineering practices that are specifically designed for mission critical systems.*

2. *The development process must produce comprehensive and objective evidence that the systems are secure and reliable.*

3. *Electoral commissions must be given the necessary resources to establish, implement and manage best practice e-election systems development.*

Recommendation 2. *E-election systems and the development processes employed must undergo rigorous audits conducted by a range of independent experts with extensive knowledge and experience covering areas including security, software engineering, mission critical systems and election technology.*

Recommendation 3. *All e-election systems must have comprehensive and ongoing risk assessments that examine the full range and extent of the risks to election security and reliability. The assessments must consider the technologies, procedures and policies associated with these systems.*

Recommendation 4. *Risk assessments for all e-election systems must involve broad consultation and collaboration with independent experts, electoral commission staff at all levels, and the general public.*

Recommendation 5. *The source code and all associated documentation, manuals and reports for e-election systems must be published on electoral commission websites.*

Recommendation 6. *All projects for e-election systems must mandate that:*

1. *electoral commissions retain total control over the development and operation of the systems, and*

2. *the full details of the systems and the development and auditing processes will be made public.*

Recommendation 7. *All electoral commissions should engage in high level consultations with privacy commissioners to consider the following measures for ensuring the transparency of electoral roll data:*

1. *publishing lists of all the types of personal information stored and collected,*

2. *publishing live disclosure logs for third party data collection and distribution events, which list the purposes, the third parties, the precise categories of voters involved, and all the types of personal information involved,*

3. *notifying voters whenever any of their personal information is updated or distributed to a third party, and*

4. *providing a service for voters to inspect and amend the personal information stored on them, including all secondary information.*

1 Introduction

Elections in Australia are heavily reliant on e-election systems. At present many electoral commissions are upgrading their existing systems and developing new systems to streamline or replace manual processes. In particular this new generation of e-election systems is intended to enable greater online access for both voters and staff. But the current paradigm for developing these systems follows standard IT industry practices, which are dangerously deficient for critical systems and have caused numerous problems with the e-election systems now in use.

For example prior to the 2010 Federal election, the AEC rolled out several new e-election systems including:

1. GENESIS (General Enrolment, Elections Support and Information System) for electoral roll management,
2. ORS (Online Recruitment System) for managing the recruitment of polling officials,
3. Checkpoint online training for polling officials, and
4. SmartForm online enrolment applications.

All these suffered from serious failures leading up to the election. Although some were briefly mentioned in the AEC's submission (AEC, 2011), the CPSU's submission observed a larger set of problems (CPSU, 2011). These included poor performance, poor usability, missing functionality and glitches such as freezes, crashes and outages.

In addition the CPSU's submission reported multiple shortcomings in the processes for developing these systems. The testing was inadequate, as was the training for both staff using the systems and staff supporting the systems at help desk. Many significant issues raised by staff were ignored or were not dealt with properly and/or in a sufficiently timely manner. Also the projects experienced multiple delays, which resulted in bad timing in launching some of the systems close to the election.

These incidents reflect the need to establish and implement best practice for developing, managing and scrutinising e-election systems. This exceeds best practice for general IT systems due to the critical nature and unique requirements of elections.

In this submission we examine changes that are required to achieve best practice for e-election systems. We cover practices in three areas:

1. development and auditing,
2. risk assessments, and
3. transparency.

Most of our comments are general in nature and predominantly deal with high level procedural and cultural changes. Concrete solutions will require open discussion and broad consultation, with input from both experts and the general public.

2 Development and Auditing

E-election systems are mission critical systems where security and reliability are paramount. In contrast to regular IT systems, mission critical systems require strong assurances that the systems meet the highest standard. Providing such guarantees demands the use of rigorous development methodologies (by development we also include testing, deployment and maintenance) and rigorous auditing.

2.1 Rigorous Development Methodologies

E-election systems are currently developed using conventional practices that do not place sufficient emphasis on avoiding the introduction of defects into the system, and instead are overly dependent on testing to eliminate system defects. This is highly problematic because the complexity of IT systems makes it easy to introduce defects, and at the same time makes it almost impossible to detect all the defects through testing. As a result it is common for critical production systems to contain bugs that remain undiscovered until they cause failures during live operation.

For example the ACT e-counting system suffered from failures during the 2001 ACT Legislative Assembly Election, and this led to delays in publishing the final result (Canberra Times, 2001). Similarly the NSW e-counting system experienced irrecoverable crashes during the 2003 NSW State Election (NSWSEO, 2005). Both these systems had undergone extensive testing and the problems were caused by relatively minor defects. The NSW Electoral Commission acknowledged that it lacked the expertise and resources to develop its e-counting system as a mission critical system.

To ensure the security and reliability of e-election systems, the development process must employ a rigorous engineering approach that minimises defects from being introduced, systematically identifies and eliminates defects, and demonstrates the system is bug free. Best practice software engineering techniques and processes have proven to be successful in developing the highest quality IT systems. These have become mandatory practice for mission critical systems such as avionics and medical equipment, and they have even become standard practice for developing computer *hardware* because any flaws are extremely expensive to rectify. We must apply the same methodologies to developing e-election systems.

Recommendation 1. *E-election systems must be developed using best practices for mission critical systems rather than standard practices for commercial IT systems.*

1. *The development process must use rigorous, well-established software engineering practices that are specifically designed for mission critical systems.*

2. *The development process must produce comprehensive and objective evidence that the systems are secure and reliable.*

3. *Electoral commissions must be given the necessary resources to establish, implement and manage best practice e-election systems development.*

2.2 Rigorous Audits

Rigorous audits conducted by independent experts are also integral to assuring the high quality of e-election systems. Audits for mission critical systems require substantial time, resources and expertise to evaluate both the systems and the development processes.

However in many instances the auditing process is not given sufficient care and attention. For example auditing was not considered at all for the NSW e-counting system discussed above. In the case of the NSW iVote system, the feasibility study originally scheduled less than eight days in total for conducting the audit and addressing the findings, with the voting period commencing ten days later (NSWEC, 2010). This was despite the fact that iVote was claimed by the vendor as being "[a]rguably the world's most far reaching and advanced remote voting solution ever to be offered for a government election" (Everyone Counts, 2011b).

It would be unreasonable to expect that major flaws with such a complex system could be discovered and fixed in such a short time frame, and undoubtedly this would place the auditor under enormous pressure not to find problems. Moreover had there been adverse findings, the NSW Electoral Commission would have been conflicted in deciding whether to proceed with using a highly vulnerable system in a mission critical environment, or to abandon the system and potentially disfranchise 50000 voters who planned to use iVote (note that voter registration for iVote was scheduled to open two weeks before the audit was due to be completed).

In addition it is common for auditors to lack the necessary expertise and experience. For instance the ACT e-counting system was certified by an independent auditor but still had defects that caused failures during an election. Also the auditor failed to identify other defects that could cause incorrect election results and system crashes. These were elementary bugs that could have been detected using standard testing methods and very simple test cases. The defects were later discovered by researchers from the Australian National University (Goré, 2004).

Knowledge and expertise is notably lacking in current security audits, which frequently overlook many of the threats and vulnerabilities that are unique to e-election systems. E-voting security expert Doug Jones suggests that "many of today's security professionals have focused so much on conventional data processing applications using Microsoft Windows in a corporate setting that they are very poorly adapted to examining the security of novel applications outside the Windows domain or outside the commercial data processing domain" (Jones, 2004).

As an example the remote voting system for the ADF trial in the 2007 Federal Election had potential security and vote privacy vulnerabilities that were not considered by the auditor (CORE, 2008). Furthermore this had long term consequences extending beyond the ADF trial as NSW later used the same vendor and core system for its iVote project. If the ADF audit had identified the fundamental flaws with the system, then it seems likely that NSW would have chosen a superior system for iVote.

Even when well-known security vulnerabilities have been identified, a poor understanding of their significance has led to inaction. For example the e-voting system for the 2010 Victorian State Election used a weak, non-standard method for seeding pseudorandom

number generators for some cryptographic keys (CORE, 2010). Both the auditor and vendor dismissed this issue as being negligible (BMM, 2010; Scytl, 2011), even though it belongs to a well-known class of security vulnerabilities and such weaknesses have been exploited in other systems, for instance the Netscape SSL attack (Goldberg and Wagner, 1996). Disregarding such flaws is contrary to what is expected for audits of mission critical systems.

Given the large number and diversity of complex issues that need to be examined, we must ensure that broad and deep audits of e-election systems are carried out with the collaboration of multiple experts whose combined specialist knowledge encompasses all areas concerned.

Recommendation 2. *E-election systems and the development processes employed must undergo rigorous audits conducted by a range of independent experts with extensive knowledge and experience covering areas including security, software engineering, mission critical systems and election technology.*

3 Risk Assessments

The critical role of e-election systems in the democratic process means there is a high risk that faults and vulnerabilities can have extensive and catastrophic consequences. To understand these risks, it is essential to conduct risk assessments that are comprehensive and involve broad consultation. This enables well-informed decisions to be made about whether to commission a system in the first place, and then if so what technical and procedural safeguards must be part of the system design from the outset.

3.1 Comprehensive Risk Assessments

Risk assessments for e-election systems currently focus on the business case, paying close attention to risks such as cost blowouts, delays in delivery and failing to realise the expected benefits. But they typically do not give due consideration to the full range of concerns over election security and reliability. This has resulted in overly ambitious practices that disregard well-known, foreseeable IT risks.

For example it has become the norm for new e-election systems to be developed on a tight schedule and then to be deployed at the most crucial point of the electoral cycle. Given that this leaves little margin for error and that IT projects have the propensity to be delayed, there is a large risk of compromising the quality of these systems. This was the case with the NSW iVote project, where development started only six months before the election. The Internet voting system ended up omitting core functionality such as providing audio instructions for visually impaired voters.

Likewise several new systems developed by the AEC for the 2010 Federal Election were launched in the lead up to the election, even after multiple flaws were identified with these systems. This caused numerous difficulties for AEC staff and required temporary workarounds to counter problems with the systems. Such risk prone practices are inappropriate for mission critical systems.

Additionally there is a particular tendency to overlook or underestimate security risks. In many cases risk assessments only account for immediate threats and vulnerabilities, instead of also anticipating eventual threats and vulnerabilities that are expected in the future. For example the AEC was under the impression that the Senate counting system was secure because it operated on a standalone machine (AEC, 2003, footnote 41, p 25). But the counting system was in fact designed to have the capability to operate in a networked environment (AEC, 2003, paragraph 8.5), which is in line with the trend to integrate all e-election systems, to expand interoperability and to open many systems directly to interaction through the Internet. In such cases the initial incorrect risk assessments can cause e-election systems to be permanently exposed to higher risk because there may be limited scope to later apply suitable countermeasures to intrinsically insecure systems.

Furthermore sudden changes to a system can drastically alter the risk profile. For instance the NSW iVote system was originally restricted to a small group of voters but was later expanded to include interstate and overseas voters. As a result of this major change in scope almost 50000 votes were cast over the Internet, which was ten times the number anticipated and posed substantially greater risks. Even in one of the largest landslide elections in Australian history, this could still have had potentially devastating impacts in affecting important outcomes, most notably the result in the tightly contested seat of Balmain. In much closer elections such as the 2010 Federal Election, similar scope changes could have implications for the integrity of overall election results.

Therefore careful and continual risk assessments that emphasise election quality must form the basis for all decisions about commissioning the development of new e-election systems, or upgrades and modifications to existing systems including their intended usage. These assessments need to follow best practice for e-election systems and exceed standards such as AS/NZS ISO 27001 (Information Security Management Systems), which only specify minimum acceptable practice for general IT systems.

Recommendation 3. *All e-election systems must have comprehensive and ongoing risk assessments that examine the full range and extent of the risks to election security and reliability. The assessments must consider the technologies, procedures and policies associated with these systems.*

3.2 Broad Consultation

Risk assessments are usually conducted by senior management staff in electoral commissions and sometimes in conjunction with external consultants. However a more open and collaborative approach is required. The CPSU's submission (CPSU, 2011) demonstrates that front line staff who use and support e-election systems are among the most qualified to identify potential practical issues, and so risk assessments must consult electoral commission staff at all levels. Also it is vital to engage multiple independent experts in the same way as rigorous auditing, given the complex and diverse risks associated with e-election systems.

Most important though is the need for public consultation. E-election systems can

have serious irreversible and far-reaching implications, which may extend beyond the electoral realm and into the public sphere, and the risks warrant open discussion.

A prominent example is the privacy implications of e-election systems related to the electoral roll. NSW and Victoria have recently introduced automatic enrolment systems, and these continue the expansion of function creep in electronic electoral roll systems, where a series of seemingly minor and insignificant changes has ended up having a massive compound effect.

The increasingly large volume and variety of data collected for the electoral roll has not only amplified the scale of the risks of violating the privacy of personal voter information but has also changed the very nature of the risks. Leaking this highly sensitive roll data can now have extremely harmful consequences including identity fraud. Also the introduction of systems such as electronic certified lists has created greater scope for roll data to be leaked through loss or theft.

This highlights the dilemma where on the one hand electoral commissions are under pressure to develop e-election systems to improve the democratic process; but on the other these systems may unexpectedly come into conflict with the public interest because they have wide ranging risks that can significantly impact the everyday lives of voters. Consequently the public must always be involved with the risk assessment process to ensure electoral commissions understand these concerns and take proactive steps to mitigate the broad risks.

Recommendation 4. *Risk assessments for all e-election systems must involve broad consultation and collaboration with independent experts, electoral commission staff at all levels, and the general public.*

4 Transparency

Transparency is a well-established democratic principle that has a fundamental role in assuring and enhancing the integrity of elections. But so far the use of e-election systems has substantially eroded election transparency and thereby the public's ability to comprehend and scrutinise the electoral process. Transparency in e-election systems can only be achieved by applying the highest level of disclosure, and this must exceed the levels of disclosure currently applied to manual and paper-based election systems because of the difficulties in understanding how electronic systems operate and determining if they are operating correctly.

4.1 Public Scrutiny

The current lack of transparency in e-election systems prevents thorough public scrutiny and parliamentary oversight of many aspects of elections. There is scant information on what e-elections systems are used, how they operate and what problems were encountered during elections, even in electoral commission reports to parliamentary inquiries.

For example most of the public details regarding problems with the new e-election systems used in the 2010 Federal Election came to light through the CPSU's submis-

sion, and it seems possible that some problems were not reported at all. Although the AEC conducted a post implementation review of these systems, this review was not transparent or subject to public scrutiny.

Electoral commissions are understandably conflicted because revealing flaws in their systems could reduce public confidence in elections, but at the same time is crucial to identifying and correcting the flaws, as well as providing accountability. This conflict can be avoided by taking proactive measures that provide full transparency of e-election systems well in advance of elections, so that the public knows the flaws have been fixed before the election.

In 2001 the ACT Electoral Commission published most of the source code for its e-voting and e-counting systems. This set a very high standard for transparency and enabled public scrutiny by researchers who discovered faults in the e-counting system, as described above. Nevertheless a greater degree of transparency is still necessary. The incomplete source code and the absence of documentation precluded a comprehensive analysis of these systems. Conducting such a study is only possible with access to all material related to the system.

However since then all e-election systems developed elsewhere in Australia have gone backwards in terms of transparency and public scrutiny. Other electoral commissions have repeatedly resisted calls to publish source code for their systems. For example the Victorian SARC Inquiry into Electronic Democracy recommended that the Victorian Electoral Commission should publish the source code for its e-counting system on its website and collect comments and bug reports from the public (SARC, 2005, Recommendation 56, p 130). But this recommendation was disregarded. Instead the VEC maintains that it is sufficient to have the system certified by an independent auditor and then to provide electronic ballot data to scrutineers, who can calculate the election result and compare it to the published results (VEC, 2005, section 2.1).

This is inadequate because certification does not promote public confidence in the system being free from bugs, considering that the audit report was never published and that the VEC engaged the same auditor who overlooked basic defects in the ACT's e-counting system. Formal audit processes must be supplemented by public scrutiny as an additional layer of defence against faults and vulnerabilities that evade detection during the audit, and against systematic flaws in the audit process itself.

Moreover giving the ballot data to scrutineers does not ensure that the counting will be thoroughly scrutinised. Political parties may lack the requisite expertise and resources to develop software to count the votes and generate all the data necessary for verifying the detailed results data published by electoral commissions. Also there is the question of what would happen if a scrutineer claimed that their counting software gave a different result. Resolving such disputes could be very difficult and time-consuming. Furthermore unique risks such as the potential to violate voter privacy in preferential electoral systems through signature attacks (Di Cosmo, 2007; Wen, 2008) must be considered before deciding if it is acceptable to disclose the ballot data.

There remains no clear best solution for guaranteeing proper scrutiny of e-counting systems, and perhaps no level of disclosure can provide such guarantees. But certainly the complete details of these systems must be made public, in order to lower the bar-

riers to public scrutiny and to enable broad discussion about what additional scrutiny measures need to be taken.

Electoral commissions already strongly encourage open, inclusive and collaborative scrutiny of many aspects of elections, for instance by publishing a wealth of material on their websites to inform the general public about how elections work. Even greater effort is necessary to provide transparency in e-election systems, which are highly complex and technical in comparison to the corresponding manual processes.

Transparency in e-election systems requires full disclosure of all related material. Only in this way will it be possible for the public to understand e-election systems and participate in the scrutiny process, regardless of their technical knowledge. For instance interested voters who are IT professionals should be able to examine technical aspects of the systems, while voters with a non-technical background should have access to expert reports and be able to directly inspect high level documentation such as user manuals.

Recommendation 5. *The source code and all associated documentation, manuals and reports for e-election systems must be published on electoral commission websites.*

4.2 Obscurity and Intellectual Property

A common argument for concealing source code and other system details is that "security through obscurity" is needed to ensure the security of e-election systems. But this is widely recognised by security experts as misguided (Mercuri and Neumann, 2003). In contrast widespread analysis of source code increases the likelihood of identifying and rectifying vulnerabilities. Indeed some vendors incorporate open source software components into their systems and are enthusiastic in promoting the benefits. The NSW iVote vendor is one example (Everyone Counts, 2011a), though their commitment to open source software did not extend to openness of the iVote source code.

Furthermore the code for closed source systems is usually distributed extensively. Electoral commissions, independent auditors and subcontractors working for these organisations will typically have access to the source code. In addition vendors have other clients ranging from foreign governments to private organisations and political parties, and these clients may also have access to the code. These clients would have greater knowledge of our e-election systems' vulnerabilities than the Australian public, and motivated attackers could obtain this knowledge without much difficulty.

The wide distribution of the source code also poses substantial risk that the code will be leaked further. For example source code for e-election systems developed by Diebold (a US vendor) was leaked on two separate occasions. The first leak was due to poor security practice where Diebold's own staff stored the code on insecure public servers. This code was discovered through a Google search and then published on the Internet, which led to serious security vulnerabilities being publicly exposed (Jones, 2003; Kohno et al., 2004). The second leak was apparently a deliberate act by a staff member working for an independent auditor (Rubin, 2006).

In reality intellectual property issues are behind the reluctance to disclose details about e-election systems: private vendors want to protect their core products, which are their

primary assets. This means independent experts and auditors who are engaged in evaluating the security and reliability of e-election systems are forced to sign non-disclosure agreements with the vendor directly (rather than with an electoral commission) in order to perform any in-depth examination, as this requires access to source code. These agreements typically prohibit any comments from being made about the system without the vendor's prior approval, and naturally this can severely limit the public disclosure of adverse findings.

More relaxed confidentiality agreements are still overly restrictive. For example the Victorian Electoral Commission engaged Dr Teague to participate in the formal audit process for the e-voting system used in the 2010 Victorian State Election. This was notable as the first instance of an Australian electoral commission collaborating with an independent e-voting expert to review an e-election system. But at the vendor's insistence, Dr Teague was required to sign a confidentiality agreement that did not allow access to source code and only permitted access to limited documentation with the proviso that it had to be viewed in person at the VEC's office. Such onerous and inconvenient conditions discourage active involvement in the scrutiny process and also effectively preclude wider involvement by the public. This scenario could and should have been avoided by requiring openness as a non-negotiable condition of the initial tender and contract rather than placing it at the vendor's discretion. Indeed, the vendor has demonstrated that it is perfectly capable of publishing source code when it is mandated by the client (Gjøsteen, 2010; Scytl, 2011).

As the procurement of e-election systems through outsourcing or as commercial off-the-shelf software is becoming more commonplace, especially for specialised systems such as e-voting systems, obscurity is even causing difficulties for electoral commissions themselves. In these situations electoral commissions typically have minimal or no oversight over the development process and may not even be able to determine how the systems function, let alone evaluate the quality of the systems.

A Dutch case study has shown that these problems with outsourcing can lead to a loss of ownership and control over parts of the election process (Oostveen, 2010). There is already evidence of this happening in Australia. For example the AEC's Checkpoint online training system for polling officials was procured through a private vendor. The Checkpoint website was operated by the vendor, which would have meant the AEC had no control over the system's availability, performance and stability, and was limited in the level of in-house help desk support that it could provide its own staff.

The push to harness e-election systems and their benefits has allowed commercial interests to override transparency. The consequent obscurity has prevented the public, experts, parliaments and electoral commissions alike from thoroughly scrutinising, overseeing and protecting election integrity. At the same time obscurity has not prevented attackers from gaining the knowledge required to exploit system vulnerabilities. We need to change this current approach to procuring e-election systems by guaranteeing that transparency cannot be compromised.

Recommendation 6. *All projects for e-election systems must mandate that:*

1. *electoral commissions retain total control over the development and operation of*

the systems, and

2. *the full details of the systems and the development and auditing processes will be made public.*

4.3 Transparency of Electoral Roll Data

Electronic electoral roll systems have greatly enhanced the capabilities of electoral commissions to collect an immense volume and variety of personal voter information from a wide range of sources. But there remains poor transparency over the amount and types (such as date of birth, occupation and phone numbers) of information gathered and stored on the electoral roll (the term 'roll' is used here to include the main roll database and all associated electoral commission databases containing personal voter information). Although members of the public can inspect the public components of the electoral roll, they do not have any means to verify all their personal information or even to identify exactly which types of secondary information are collected or maintained.

At the same time a growing number of third parties has been granted access to the roll, and this includes access to more types of secondary information. This has been a consequence of the continually advancing data collection and data matching systems used to increase the quality, quantity and variety of personal information stored on the roll, which has made the roll an extremely valuable and attractive information source. But again there is minimal transparency over what, when, why and to whom roll data is provided. It has thus become extraordinarily difficult for the public to track the flow of their personal information to third parties.

To complicate the problem third parties, which include political parties, private corporations, medical researchers and other government agencies (including other electoral commissions), may have weak policies or legislative restrictions on how they use the obtained data and what data they can publish or distribute to other third parties. This further obfuscates what subsequently happens to personal voter information.

Third parties may also have conflicts of interest. For example the AEC regularly distributes roll data to certain private corporations for ostensibly legitimate reasons such as to detect money-laundering (AEC, 2010, Appendix F, Table 57). But as part of their core business some of these companies offer marketing services including direct marketing and the sale of marketing lists. Without public awareness of what roll data has been provided, it is almost impossible for individuals to discover if their personal voter information is being improperly used for such purposes.

Despite having little control over which third parties are authorised to obtain roll data and what degree of transparency these third parties provide, as the originating source of this personal information electoral commissions have an enormous responsibility to ensure full transparency of all their own actions. This is the first step towards untangling the web of personal information flow and guaranteeing the accountability of all organisations that possess roll data.

These issues are among long-standing concerns raised on numerous occasions, for instance by the Federal Privacy Commissioner at the JSCEM Inquiry into the 2001

Federal Election (OFPC, 2002a; OFPC, 2002b; OFPC, 2002c) and the JSCEM Inquiry into the Integrity of the Electoral Roll (OFPC, 2000). More recently an ANAO audit voiced similar concerns and recommended that the AEC undertake a review of the many privacy issues related to the roll with the assistance of the Federal Privacy Commissioner (ANAO, 2010, Recommendation 1, paragraph 2.28).

This is a positive step and all electoral commissions should carry out similar reviews. However in doing so it is essential to recognise the outdated and ineffective nature of existing privacy legislation such as the *Privacy Act 1988*, which is presently the subject of detailed reform. Best practice measures for providing transparency must go far beyond the minimum requirements of the Privacy Act and should instead strive to follow the spirit and intent of the Act. Particular consideration should be given to timely and detailed disclosure of both data collection and data distribution events.

Recommendation 7. *All electoral commissions should engage in high level consultations with privacy commissioners to consider the following measures for ensuring the transparency of electoral roll data:*

1. *publishing lists of all the types of personal information stored and collected,*
2. *publishing live disclosure logs for third party data collection and distribution events, which list the purposes, the third parties, the precise categories of voters involved, and all the types of personal information involved,*
3. *notifying voters whenever any of their personal information is updated or distributed to a third party, and*
4. *providing a service for voters to inspect and amend the personal information stored on them, including all secondary information.*

References

AEC (2003). *Submission 181 (supplementary), Inquiry into the 2001 Federal Election*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.aph.gov.au/house/committee/em/elect01/subs/sub181.pdf.

AEC (2010). *Annual Report 2009–2010*. URL: http://www.aec.gov.au/About_AEC/Publications/Annual_Reports/files/aec-annual-report-2009-10.pdf.

AEC (2011). *Submission 87, Inquiry into the 2010 Federal Election*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.aph.gov.au/house/committee/em/elect10/subs/Sub087.pdf.

ANAO (2010). *The Australian Electoral Commission's Preparation for and Conduct of the 2007 Federal General Election*. Audit Report No. 28 2009–1010. URL: http://anao.gov.au/~/media/Uploads/Documents/2009%2010_audit_report_28.pdf.

BMM (2010). *Electronically Assisted Voting Audit*. URL: http://www.vec.vic.gov.au/files/EAV-BMM-Report.pdf.

Canberra Times (29th Oct. 2001). *Libs set to take third seat in Molonglo*. URL: http://www.canberratimes.com.au/news/local/news/politics/libs-set-to-take-third-seat-in-molonglo/157026.aspx.

CORE (2008). *Submission 116.1 (supplementary), Inquiry into the 2007 Federal Election*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.aph.gov.au/house/committee/em/elect07/subs/sub116_1.pdf.

CORE (2010). *Report on the VEC-Scytl Electronic Voting System for the 2010 Victorian Election*. URL: http://www.vec.vic.gov.au/files/EAV-CORE-Report.pdf.

CORE (2011). *Submission 101, Inquiry into the 2010 Federal Election*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.aph.gov.au/house/committee/em/elect10/subs/Sub101.pdf.

CPSU (2011). *Submission 95, Inquiry into the 2010 Federal Election*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.aph.gov.au/house/committee/em/elect10/subs/Sub095.pdf.

Di Cosmo, Roberto (2007). 'On Privacy and Anonymity in Electronic and Non Electronic Voting: the Ballot-As-Signature Attack'. URL: http://www.pps.jussieu.fr/~dicosmo/E-Vote/.

Everyone Counts (2011a). *eLect Platform*. URL: http://www.everyonecounts.com/index.php/elections/elect_platform.

Everyone Counts (15th Apr. 2011b). *New Remote Voting Solution is Largest Implementation in History for Voters with Disabilities*. URL: http://www.everyonecounts.com/index.php/news/99/95/New-Remote-Voting-Solution-is-Largest-Implementation-in-History-for-Voters-with-Disabilities.

Gjøsteen, Kristian (2010). *Analysis of an internet voting protocol*. Cryptology ePrint Archive, Report 2010/380. URL: http://eprint.iacr.org/.

Goldberg, Ian and Wagner, David (1st Jan. 1996). *Randomness and the Netscape Browser*. Dr. Dobb's Journal. URL: http://drdobbs.com/architecture-and-design/184409807.

Goré, Rajeev P. (2004). *Electronic Voting - A Review of the Hare-Clark Model of eVACS*. URL: http://users.cecs.anu.edu.au/~rpg/EVoting/evote_revacs.html.

Jones, Douglas W. (2003). *The Case of the Diebold FTP Site*. URL: http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html.

Jones, Douglas W. (2004). 'Misassessment of Security in Computer-Based Election Systems'. In: *CryptoBytes* 7.2, pp. 8–12. URL: http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_Fall2004.pdf.

Kohno, Tadayoshi et al. (2004). 'Analysis of an Electronic Voting System'. In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, pp. 27–.

Mercuri, Rebecca and Neumann, Peter G. (2003). 'Security by obscurity'. In: *Communications of the ACM* 46.11, p. 160.

NSWEC (2010). *Report on the Feasibility of Providing iVote Remote Electronic Voting System*. URL: http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/84498/20100723_NSWEC_iVote_Feasibility_Report_.pdf.

NSWSEO (2005). *Submission 10, Inquiry into the Administration of the 2003 NSW Election*. Parliament of New South Wales, Joint Standing Committee on Electoral

Matters. URL: http://www.parliament.nsw.gov.au/Prod/parlment/committee.nsf/0/6bd39b93036026cfca25784800104d5f/$FILE/SUB10%20-%20SEO.PDF.

OFPC (2000). *Submission 42, Inquiry into the Integrity of the Electoral Roll*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.privacy.gov.au/materials/types/download/8662/6506.

OFPC (2002a). *Submission 154, Inquiry into the 2001 Federal Election*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.aph.gov.au/house/committee/em/elect01/subs/sub154.pdf.

OFPC (2002b). *Submission 164 (supplementary), Inquiry into the 2001 Federal Election*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.aph.gov.au/house/committee/em/elect01/subs/sub164.pdf.

OFPC (2002c). *Submission 172 (supplementary), Inquiry into the 2001 Federal Election*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.aph.gov.au/house/committee/em/elect01/subs/sub172.pdf.

Oostveen, Anne-Marie (2010). 'Outsourcing Democracy: Losing Control of E-Voting in the Netherlands'. In: *Policy & Internet* 2.4, pp. 201–220. URL: http://www.psocommons.org/policyandinternet/vol2/iss4/art8.

Rubin, Aviel D. (20th Oct. 2006). *Another Diebold source code leak*. URL: http://avirubin.blogspot.com/2006/10/another-diebold-source-code-leak.html.

SARC (2005). *Final Report on the Inquiry into Electronic Democracy*. Parliament of Victoria, Scrutiny of Acts and Regulations Committee. URL: http://www.parliament.vic.gov.au/archive/sarc/E-Democracy/Final_Report/Final_Report.pdf.

Scytl (2011). *Comments from Scytl on the CORE Report from the Electronic Voting Solution Used in 2010 Victorian Election*. URL: http://www.vec.vic.gov.au/files/EAV-Scytl-CORE-Report.pdf.

VEC (2005). *Submission 27, Inquiry into Electronic Democracy*. Parliament of Victoria, Scrutiny of Acts and Regulations Committee. URL: http://www.vec.vic.gov.au/files/RP-ElectronicDemocracy.pdf.

Wen, Roland (2008). *Submission 181, Inquiry into the 2007 Federal Election*. Parliament of Australia, Joint Standing Committee on Electoral Matters. URL: http://www.aph.gov.au/house/committee/em/elect07/subs/sub181.pdf.