Democracy and voting

By Carol Boughton MSc, FAICD, Director Software Improvements

1. Introduction

All democratic election systems have many things in common no matter where a particular system is applied.

In the UK, Watt (2002) initially identified six principles as forming the minimum requirements of a democratic election procedure (see Appendix B). Public consultations established wide community support as well as leading to their simplification to three principles:

1) the **doorkeeper** principle
   Each person desirous of voting must be personally and positively identified as an eligible voter and permitted to complete no more than the correct number of ballot papers.
2) the **secrecy** principle
   Admitted voters must be permitted to vote in secret.
3) the **verification, tally and audit** principle
   There must be some mechanism to ensure that valid votes, and only valid votes, are received and counted. This system must be sufficiently open and transparent to allow scrutiny of the votes and subsequently the working of the political process.

More recently Tokaji (2004) identified three democratic values as being essential to any voting system adopted in the USA:

i) **equality** (of political participation)
   - racial equality
   - multi-lingual access
   - disability access
   - inter-jurisdictional access (or no differential treatment to voters based on the county or jurisdiction where they reside)

ii) **security** (the resistance of votes and vote totals to fraud and other forms of manipulation), and

iii) **transparency** (the capacity to produce auditable results in which both candidates and voters can justifiably have confidence).

The values and principles identified in Watt (2002) and Tokaji (2004) of **equality**, **secrecy**, **security** and **transparency**, apply to any democratic election system – no matter whether the election is conducted using paper ballots, mechanical or electronic means.

Exactly these requirements were specified for the electronic voting and counting system - eVACS® developed by Software Improvements for the Australian Capital Territory Electoral Commission (include here hyperlink to Credible Election Software paper).

2. eVACS® means Equality

eVACS® includes a number of features to enable voters who normally require assistance to vote by themselves and thereby have a secret vote.

For vision impaired voters or voters with poor reading skills using eVACS®, audio is activated and, if required, a larger screen provided. Privacy is maintained by the use of a headset; voters can use their own headset or a disposable headset.

The use of a (special) keypad by a voter to record their choices/preferences enables voters with a range of physical impairments to vote without assistance. In preferential or proportional systems eVACS® ensures people accurately record a sequence of preference numbers without missing or repeating numbers.

Instructions are provided in the voter's language of choice, as well as the local language of the region, using any alphabet or character set.

If permissible by law, voters are able to vote away from their normal polling place.

3. eVACS® means Secrecy

The eVACS® voting system maintains voter secrecy in five ways whilst allowing the voter to either sit or stand to vote:

i) the voting screen is positioned so that no other person is able to see a constructed vote;
ii) the system fits in a normal cardboard voting booth;
iii) for the standard arrangement eVACS® emits no noise signals to alert anyone else as to how a voter may be voting;
iv) because voters navigate the 'electronic ballot' it is extremely difficult for anyone else to be able to discern who is being voted for; and
v) eVACS® enables a voter to 'hide their vote' if they need to seek assistance from an official.

In addition, all of the eVACS® equality features increase the number of people who can vote without assistance, and thereby vote in secret.

4. eVACS® means Security

Security in eVACS® involves a number of design and operational aspects covering software and hardware.

Features include:

i) automated set-up arrangements ensure that an election is run from a series of auditable write once CDs;
ii) limited functionality available to voters and officials means software cannot be modified during an election;
iii) on loading eVACS® the hard disk/s are reformatted thereby removing any existing operating system and other software;
iv) barcode determines in which election/s voter is eligible to vote;
v) whether barcode has been used is checked by eVACS® before voting commences;
vi) barcode ensures only completed votes are stored;
vii) whether barcode has been used can also be checked manually;
viii) generation of a restricted set of barcodes within eVACS®;
ix) protection of completed votes and identification of incomplete votes if the network is disrupted;
x) outcome of a rerun in sequential order of voter keystrokes must match with the voter's choices before vote is recorded;
xi) all votes are cast in a public polling place over an isolated LAN;
xii) votes only stored on physically secure voting servers; no votes stored on voting machines used by voters;
xiii) votes stored in two separate databases to guard against hardware failure;
xiv) log of all activities;
xv) downloading of votes at end of polling requires password and encryption keys, not transmitted to polling place officials until after polling closes; and
xvi) votes are encrypted and downloaded to two write once CDs with checksum; both disks have to be loaded into counting server and match with checksum.

Auditing and internal security features of eVACS® ensure a court is able to verify the CDs that were used for a specific election, and that the election result is accurate and has not been tampered with in any way.

4.1. Security of hardware

eVACS® is designed to run on any hardware which supports the Linux operating system. The degree of in-built security of hardware can vary significantly between equipment. Consequently, eVACS® has an emphasis on maximising security via the software with physical security an added feature where available.

The Entech Group designed a rugged voting machine that was used in the 2004 ACT Legislative Assembly Election (http://www.elections.act.gov.au/Elecvote.html and http://www.roc-solid.com/). The ROC-solid voting terminals provide advantages over standard PCs in respect of ease of set-up and use, as well as better protection against external damage from liquids, solids, heat and physical damage. The LAN network is also physically protected against attempts to break into the system.

5. eVACS® means Transparency

Traditionally transparency is managed by having observers/scrutineers present at different stages of the voting and counting processes, such as:

- empty ballot box and then securing (eg by sealing or locking) the box at the start of polling,
- ballot boxes remaining secured until after close of poll,
- only those people who actually attend the polling place are marked off the electoral roll at that polling place,
- assistance to voters incapable of marking their ballot paper by themselves,
- only voters place the appropriate ballot papers in the ballot box during polling,
- emptying of ballot box at the close of polling,
- counting of ballot papers after close of poll,
- secure transportation and/or storage of the votes, and
- recounting of votes.

Electronic voting and counting must, by necessity, change the nature of scrutineering, but computerising the voting and counting processes ought not prevent elections from being transparent, nor prevent scrutineers from observing all aspects of the voting and counting processes (after Green (2003)).

Also, as Green (2003) writes "A computerised voting and/or counting system is in essence a series of mechanical steps, facilitated by computer hardware and computer programs. A thorough understanding of the way in which the hardware and programs work – the electronic trail – should serve to demonstrate that the system is transparent, and in particular, that 'what goes in is what comes out'."

There are some activities of scrutineering that are outside the scope of electronic voting and counting. To ensure the anonymity of votes there can be no connection between the voter's details and their vote. Any system for marking people off the electoral roll (either paper or electronic) must be independent of the voting and counting processes. Hence, the observation process to ensure only eligible people vote continues independently of eVACS®.

As with paper ballots, transparency in an electronic election has a number of stages, or levels, none of which is sufficient by itself to demonstrate the required transparency for an election. eVACS® was designed and implemented to ensure all of these levels of transparency are completely fulfilled (Table 1).

In addition, there is a well-documented 'electronic trail' for eVACS®. All the development artefacts and code were made available to an independent auditor (engaged by the customer not Software Improvements), the compiled code underwent extensive testing, and the source code published for examination by interested persons.

Table 1 – Ensuring transparency of the election processes with eVACS®

Level of Transparency	Requirement	Transparency with eVACS®
First	Availability of software code so others can assure themselves that the software does what it is meant to do and nothing else.	• Source code for eVACS® was released under the GNU GPL, enabling people with the skills to assess and assure others that the code operates as required. • eVACS® as provided for acceptance testing was independently audited in 2001, and again in 2004 after enhancements were made. • Auditing arranged by the customer with Software Improvements having no contact with the auditor. • The customer certified the audited software as the software to be used for the election. • After the 2001 election, researchers from the Australian National University independently verified the counting algorithm and replicated the results of the 2001 ACT Assembly election.
Second	Correct operation of the vote recording process. Correct operation of the paper ballot data entry process. Votes counted accurately according to election system.	• Extensive testing prior to the software being put into service was undertaken. • Extensive testing of eVACS® by the customer was undertaken prior to auditing of the software. • Representatives from political parties and disability groups observed the acceptance testing.
Third	The software used for an election can be shown to be exactly the same software that passed first and second levels.	• eVACS® is version controlled and access to the master CDs is logged by the customer. • The version provided for auditing was made available to the auditor by the customer not Software Improvements.
Fourth	Officials are able to demonstrate: i) software cannot be tampered with during use in an election, ii) empty electronic ballot box at start of election iii) number of votes (formal/informal) in electronic ballot box, iv) initial results (for specific polling places), v) secure downloading of votes.	• In-built features of eVACS® ensure that the system is a closed system with limited functionality and cannot be modified during operations. • Empty ballot box can be demonstrated at start of session. • Number of barcodes recorded as used in eVACS® can be compared with number of electronic votes and number of barcodes issued. • Downloading of votes is security controlled both to download and when uploading into counting server with encryption of votes, password access and checksums on CDs.
Fifth	Voters and officials are confident that none of the recorded votes are lost, and that only completed votes are recorded.	• Each voter is provided with a bar code (based on but in no way linked to the voter's residential address), which determines in which elections the voter may vote. The bar code starts and ends a voting session. • eVACS® allows officials to check whether a bar code has been used to end a voting session. • Use of the bar code at the end of a voting session generates an automatic comparison of i) the bar code used to commence the voting session, and ii) the voter's choices (as confirmed by the voter by use of the bar code) with the outcome generated by rerunning in order the sequence of all the voter's keystrokes. Only when these match with the voter's choices will the vote details be recorded in the 'electronic ballot box'.

Dr Amy McGrath (2001) in her discussion on the introduction of computer technology as applied to electoral matters in Australia, quotes the then Commonwealth electoral authority's explanation for its reluctance to move too rapidly into computers in 1982 as follows:

It is absolutely essential not only that an election system be fair, but that it is seen to be fair. The safeguards built into the current system are the product of many years of experience. The full-scale introduction of a new, and much more complicated system could create opportunities for illicit interference, or allegations of such interference, with the electoral process. A completely new security process would have to be developed – one which would be acceptable to the electorate, the candidates and the political parties. (op cit Hansard V.129 1982 1614).

While new steps in computerisation of the election process have subsequently been taken each year, they have not been submitted, step by step, to parties and candidates for open debate, let alone to the electorate (page 166 McGrath (2001).

In Ireland the Commission on Electronic Voting (http://www.cev.ie/htm/report/first_report/pdf/00Index.pdf) in its first report (December 2004) was unable to recommend use of the chosen electronic voting system because the accuracy and security could not be established as:

i) there was not sufficient time to fully test the system,
ii) the full source code had not been made available,
iii) the version to be used was unknown and therefore the accuracy of the system could not be certified,

and there were concerns that secrecy of the vote might be compromised.

In marked contrast, the development and introduction of electronic voting and counting in the Australian Capital Territory occurred with public participation. eVACS® was:

i) developed after direct public consultation had led to legislative changes to enable electronic voting and counting,
ii) undertaken in association with a Reference Group (with representatives of candidates, political parties and the public) whose members were able to participate in the acceptance testing, and
iii) the source code released for public scrutiny before use in an election.

Apart from ensuring a completely transparent electronic trail, eVACS® also eliminates opportunities to tamper with election results as is reported occurring with paper ballots:

- ballot box stuffing:
  - Electronic votes cannot be prepared in advance; voting must occur at the polling place and under the direct observation of others.
  - The period when electronic voting is available at any polling place is logged within eVACS® by recording the times whenever the system is activated (start voting) or deactivated (stop voting).
  - A unique barcode must be obtained for each electronic vote.

- completed ballot papers from a polling place get "lost":
  - Electronic votes are stored in duplicate on the voting server at a polling place. The votes are downloaded twice onto separate write once CD-ROMs with a checksum. Details from both CDs are loaded into the counting server and confirmed with the checksum before the votes are added to the counting database.
  - The only option for downloading votes is to download all votes stored on the voting server.
  - Votes for a particular polling place can only be added once to the counting database.
  - A report is available of polling places from which votes have not been imported into the counting database.

- completed paper ballots deliberately inserted in the wrong stacks for counting:
    - Once confirmed by a voter, the limitation on the functionality of eVACS® means there is no way to interfere with the content of an electronic vote.
    - There is no means to change the counting program used to count any electronic vote once a specific election has been set-up.

5.1. Recounts and petitions

Recounts were introduced to address the known failings with manual counting of votes, and usually occur when the result of an election is very close. Either the electoral agency or a candidate may seek to have the votes recounted.

In some jurisdictions there is a mandatory requirement to recount a proportion of all votes to check the accuracy of the manual count. Whereas is other jurisdictions, a candidate, a voter or the electoral agency may dispute the validity of an election via a petition to a court.

Electronic voting and counting has significant impact on the conduct of recounts and for contesting election outcomes in the courts.

The demonstrable accuracy of electronic voting and counting with eVACS® avoids the unnecessary recounts when election results are close. Mandated recounts are not practical with eVACS®, although a random set of votes could be printed and counted manually with less accuracy.

With petitions, the issues are not ones of ‘who did or did not do what’ or ‘what was permissible under the election legislation’ but whether the computer program used met the appropriate standard of accuracy, reliability and trust. The transparency of eVACS® enables a court to independently establish the accuracy, reliability and trust in eVACS®

5.2. Electronic voting and voter verifiable audit trails

There is no question about the need for voter verifiable audit trails with electronic voting. However, as per Tokaji (2004), a ‘voter verifiable audit trail’ is not synonymous with ‘*paper* ballot replicas’.

Voter verifiable *paper* audit trails are often cited as the solution to addressing problems encountered with electronic voting in the USA. Yet as Tokaji (2004) and Elections ACT (2005) have shown, whether a voter verifiable paper audit trail is both a practical solution and an effective means of preventing fraud is highly questionable. A recent publication from electionline.org (2005), contains a photograph of the tape from a voter verifiable paper audit trail system used in Clark County, Nevada, USA. The tape, containing 64 voter verifiable paper ballots from one voting machine, is a strip of four inch wide paper, just under 120 metres in length (318 feet) and “it took a four person team - one counting votes, one verifying and checking for errors and two recording results – about four hours to check one tape, or nearly four minutes per ballot”. The ability of election officials to accurately determine election results under such circumstances becomes a costly exercise in checking and cross checking.

The USA is not the only country where concerns have been raised about the electronic voting system used. (see Rezende (2003) for comments on the system used in Brazil and the Ireland Committee on Electronic Voting (2004) regarding the NEDAP Powervote system trialed in Ireland).

There are some, for example Mercuri (2001), who believe no electronic voting system can be trusted and therefore a paper audit trail is absolutely essential. Yet Tokaji (2004) cautions against sacrificing the voting rights of disabled voters and non-English speaking citizens in order to achieve the admirable goal of enhancing election security and transparency. A voter verifiable paper audit trail is obviously not an option for the vision impaired, poor readers or voters who cannot read the language of the print out.

Not all the issues raised with electronic voting have been about ensuring votes are recorded accurately at the polling place. There have been reports of vote databases being accessed by the public, uncertified software being used, bug fixing occurring during an election, and equipment being certified without meeting certification requirements (http://www.blackboxvoting.org/). With an appropriate 'voter verifiable audit trail' none of these issues should eventuate.

All of the concerns with electronic voting have arisen where there has been no transparency of the software used nor any serious attention to security issues prior to implementation of the system.

In contrast, with eVACS® all of these issues were addressed before the system could be used in an election.

6. References

electionline.org (2005) "*Recounts: From Punch Cards to Paper Trails"*, Briefing, October 2005 http://www.electionline.org/Portals/1/Publications/ERIPBrief12_FINAL.pdf

Elections ACT (2005), "*2004 ACT Legislative Assembly Electronic Voting and Counting System Review*" ACT Electoral Commission, http://www.elections.act.gov.au/Elecvote.html

Green, Phillip (2003) the chapter on "*Transparency and Elections in Australia: The Role of Scrutineers in the Australian Electoral Process"*, in *Realising Democracy: Electoral Law in Australia*, G. Orr, B. Mercurio and G Williams (eds), The Federation Press, 2003, pages 226-228.

Ireland Commission on Electronic Voting (2004) First Report on *Secrecy, Accuracy and Testing of the Chosen Electronic Voting System,* http://www.cev.ie/htm/report/first_report/pdf/00Index.pdf

McGrath, Amy (2001), "*The Frauding of Votes*" with an Introduction by Bob Bottom, Tower Books Wholesale, ISBN 0-9587104-3-0.

Mercuri, Rebecca (2001), Rebecca Mercuri's Statement of Electronic Voting http://www.notablesoftware.com/RMstatement.html

Tokaji, Daniel P (2004), "*The Paperless Chase: Electronic Voting and Democratic Values*". Ohio State Public Law Working Paper No. 25 http://ssrn.com/abstract=594444

Watt, Bob (2002), Office of Deputy Prime Minister, UK website "*Implementing electronic voting in the UK: The legal issues*". http://www.odpm.gov.uk/index.asp?id=1133606

Rezende, Pedro AD (2003) *Electronic Voting Systems - Is Brazil ahead of its time?* Paper prepared for the First Workshop on Voter-Verifiable Election Systems Denver CO, USA July 28-29, 2003 http://www.cic.unb.br/docentes/pedro/trabs/election.htm

7. Appendices

Appendix A – Electronic votes and printed receipts

The following is a copy of Attachment A from Elections ACT (2005), and is reproduced in full with permission of the ACT Electoral Commission.

Electronic Votes and Printed Receipts

The ACT Electoral Commission has given consideration to whether there is a need to provide printed receipts of electronic votes for its electronic voting and counting system.

Much of the discussion of electronic voting in the United States of America is currently addressing whether there is a need to produce a "voter-verifiable audit trail" of electronic votes. It is suggested that this would take the form of a printed receipt that could be read by the voter (but not kept or altered by the voter) and that could be used for a manual count to verify that the computer count was accurate.

Proponents of a voter-verifiable audit trail claim that printing paper receipts would:

- Reassure voters that their vote has been correctly recorded,
- Create a disincentive to the manipulation of the system by providing an external check on accuracy,
- Enable recovery from a serious system failure; and
- Guard against computer tampering.

(See http://www.cev.ie/htm/report/part4_4.htm - Ireland's Commission on Electronic Voting, and http://www.blackboxvoting.com/ for relevant discussion.)

The ACT Electoral Commission is of the view that providing for paper receipts of electronic votes would add a layer of cost and complexity onto electronic voting without necessarily providing the expected benefits.

One of the concerns with the electronic voting systems used in the USA is the fact that the computer code used in their proprietary systems is kept secret by their vendors and not made available for public inspection or even inspection by courts in the event of a legal challenge to an election result. This, combined with a history of anomalous results, means that voters and other political participants have no way of being reassured that "what goes in is what comes out". In this context, providing for an independently-verifiable paper audit trail is a reasonable proposition.

By contrast, the ACT's electronic voting and counting system has been designed to be transparent and verifiable by making each step of the voting and counting system verifiable by public examination of the computer code used in the system, combined with a high level of physical security and the use of data verification and encryption techniques. Another feature of the system is the comprehensive testing and independent audit of the software prior to the election. The enhancements currently being implemented to eVACS® will see the entire system run from a series of auditable CD-ROMs, which could be used by a court to verify that the election result was accurate and had not been tampered with.

The checks and balances built into the electronic voting and counting system are intended to ensure that electronic votes are accurately recorded and that they cannot be lost or altered in any undetectable way. In particular:

- All votes are cast in a public polling place over an isolated local network, staffed by independent electoral officials;

- Voters are given an opportunity to review their votes (in preference order) before committing their votes to the "electronic ballot box";

- The computer program verifies that the vote recorded by the voter is correct by comparing the voter's keystrokes with the final record of the vote;

- Votes are stored in the polling place server on two identical hard disks to guard against hardware failure;

- The voter does not receive the message saying "your vote has been accepted" until after the vote has been successfully written to the two hard disks on the server – if the data is not successfully recorded the voter receives an error message that indicates the vote has not been recorded –this also guards against hardware failure;

- The software used in the polling place is loaded from CD-ROMs containing audited program code that is made available for public inspection;

- Polling place servers are physically locked away and constantly monitored by electoral officials;

- Voting data is written to write-once CD-ROMs at the end of each day's polling, with the data encrypted and identified by a "hash" number that is derived from the contents of the data – this data cannot be altered after the event without detection;

- The use of data encryption means that a greater level of security is applied to electronic votes than to paper ballots; and

- The number of electronic votes counted is compared to the number of electronic votes issued at each polling place to verify that the correct number of votes has been counted.

The ACT Electoral Commission does not consider that providing a paper receipt in addition to these measures would enhance the verifiability of the electronic voting and counting system.

Providing for a system of printing receipts that could be seen by, but not altered by, each voter in secret, would present several difficulties. For example:

- An additional item of hardware used at each voting station would add another thing that could malfunction. Printers could jam, run out of ink or run out of paper. If this happened, it might not be clear whether a vote had been successfully stored on the computer server. Printer failure would also mean that a manual count would not duplicate the computer count.

- Requiring use of a printer that displayed a printed receipt to a voter that could be removed or tampered with by the voter would involve use of non-standard hardware. Such a system might increase the cost of the electronic voting and counting system to the point that it might not be feasible for use in the ACT.

- Producing a printed receipt might violate the principle of the secrecy of the ballot by making it possible to determine how a person voted.

- It is not clear how it could be made possible for a voter to challenge a paper receipt if it did not accord with their memory of their electronic vote – presumably a paper receipt would not be printed until after the vote had been written to the computer disk. It would be difficult to implement a system where the voter was able to review a paper receipt before submitting the vote to the computer. If this was done, the paper receipts would be difficult to recount as it would be necessary to determine for each receipt whether it had been committed to the computer or not.

- A printed receipt would not by itself be proof that a person's vote had been recorded in the computer system as shown on the receipt. If a computer system was deliberately programmed to give fraudulent results, a receipt would not necessarily replicate the vote stored in the database. The only way to verify this would be to conduct a complete check count comparing the printed receipts with the electronic vote count for any given set of votes.

- Conducting a full or partial manual recount using printed paper receipts would be prone to the errors that currently beset hand counting of ballots. It is likely that a hand count of paper receipts would not be as accurate as a computer count.

- Some have argued that paper receipts should be counted by a scanner rather than by hand. Providing a separate scanning system for counting paper receipts would be an expensive add-on to the current eVACS® system. Such a system would need to be tested and audited before it could be used in production.

Taking all of these matters into account, the ACT Electoral Commission considers that paper receipts of electronic votes would not necessarily meet the needs identified above. A printed receipt would not necessarily be any guarantee that a voter could be assured that their vote was correctly recorded in the computer system. A manual recount of paper receipts would not be an efficient or effective means of recovering from a system failure. A printed receipt is also not necessarily going to be proof that a system had not been tampered with.

The ACT Electoral Commission considers that the other measures incorporated in the electronic voting and counting system will give more assurance to voters, candidates and other political participants that the votes recorded and counted are an accurate record of the voters' intentions.

Appendix B – Six principles of democratic elections

Watt, Bob (2002), identified the following six principles as essential for all democratic elections:

1) That those wishing to cast a vote are positively identified as eligible voters and that no voter is able to cast more than a single ballot in a given election;
2) That safeguards against personation are maintained;
3) That the free exercise of the vote is safeguarded, both in terms of the opportunity to cast a ballot and that voters are free from duress and unlawful undue influence;
4) That secrecy regarding how an individual elector has, or has not, voted is preserved save in the face of a proper order of a competent Court;
5) That the voting process is protected against tampering after any vote or votes have been cast; and
6) That the counting procedure is verifiable, transparent and open to scrutiny, and accurate.