

Transparency and e-Voting Democratic vs. commercial interests

Margaret McGaley, Joe McCarthy

NUI Maynooth
Computer Science Department
Co. Kildare, IRELAND
mmcgalley@cs.may.ie

Arkaon Limited
Sandymount
Dublin 4, IRELAND
joe.mccarthy@arkaon.com

Abstract: Electronic voting systems are being introduced, and have been introduced, in many countries for a variety of reasons. The introduction of computers into the electoral process can offer several advantages. Among other things it can speed up the process of calculating results, can help voters avoid accidentally spoiling their vote, and can allow voters with special needs to vote in private. Often, however, little consideration is given to the potential negative effects of electronic voting. We examine some of these negative effects in terms of the three streams of this conference: technology, law, and politics, with particular emphasis on the situation in the Republic of Ireland. The over-arching theme of this paper is that the introduction of technology into the democratic process can reduce transparency, and risks private commercial interests being given priority over public democratic interests.

1 Technology

The introduction of technology is often seen as necessary to progress, and therefore in some way unstoppable. All too often, however, little consideration is given to the new challenges - legal, political and sociological - posed by technology.

1.1 Transparency

Perhaps the greatest strength of paper voting systems is their transparency. Individual voters can satisfy themselves that the system works, because its transparency allows them to observe and understand every aspect of it. Nothing within the system is secret or impenetrable, except of course who casts which vote.

Purely electronic systems cannot offer this transparency. The nature of computers is that their inner workings are secret. Since transactions and calculations happen at an

electronic level, it is not physically possible for humans to observe exactly what a computer is doing. Once the vote is cast the voter "loses sight" of it. So if - for whatever reason - the vote is stored incorrectly, there may be no sign that something went wrong.

The change from paper to electronic records is not simply a matter of changing the storage medium. It is much more fundamental: the introduction of a computer system between voter and vote denies the voter tangible evidence that his vote has been recorded correctly. This is different from the paper system. While the voter never received evidence that he could take home, he did see the actual record of his vote (the paper ballot). Armed with the knowledge that pencil lead does not fade overnight, he could then be sure that the vote cast would be the vote counted. When the primary record of one's vote is electronic, on the other hand, one only ever sees a representation of one's vote, never the vote itself.

It is unacceptable that a voter should have to trust any agent or device to correctly relate their vote to them. Unfortunately, this is necessarily the case with purely electronic systems.

1.2 Voter Verified Paper Ballots

There is growing support worldwide [U.S, Sch00, Soc04] for the idea that 'Voter Verified Paper Ballots' (VVPBs [Mer92], also known as a 'Voter Verified Audit Trail') must be a requirement for electronic voting systems. VVPBs are paper records of the vote which have been verified by the voter at the time of casting. They might be hand-written ballots which are scanned for computer counting, or they might be printed by DRE (Direct Recording Electronic) machines in front of the voter before being deposited into a sealed ballot box [Mer02]. These paper ballots, however they were produced, would be the primary record of votes cast, since they would be the records verified by the voter. They would be used for all recounts and in a number of randomly chosen constituencies every time the system was used.

Some manufacturers of electronic voting systems, including the Nedap system being introduced in Ireland, have suggested that printing all the ballots after the close of polls would provide an equivalent audit trail. In fact this would be completely inadequate. The value added by VVPBs is that they are a record that has been confirmed correct by individual voters. If, by accident or design, the electronic records were incorrect then printed copies of those records would contain the same errors. As the old computer phrase goes - garbage in, garbage out.

Several paperless alternatives are under development [Cha04, JRB03]. However, we have yet to be convinced that any such system can provide the transparency necessary, or release voters from having to trust vendors.

The elimination of paper from elections is a significant motivating factor in the introduction of electronic voting for many governments. However, because of the nature of electronic systems, the removal of paper from voting may never be compatible with trustworthy elections.

1.3 The Nedap/Powervote System

The machines to be used in Ireland in June 2004 are classed as DRE (Direct Recording Electronic). That is, votes are cast by inputting preferences to the machine and are recorded directly to storage media within the machine. They are not touch-screen as are the majority of DRE machines used in the USA. Instead, they present the voter with a panel of buttons on which a printed sheet indicates which candidate/option is represented by each button.

Votes are stored on "ballot modules", cigarette packet sized memory cartridges. At close of poll, the contents of the main module are copied onto a backup module which remains in the voting machine unless and until needed. The main ballot modules are collected from the various polling stations and brought to a constituency count centre (in pilots undertaken so far, they were taken by taxi [Fit02]).

At the count centre the modules are read into a desktop PC¹, where the IES (Integrated Election System) count software - written in Borland Delphi and using Microsoft Access - calculates the results. The main vulnerabilities to malicious attack and/or error identified by us so far are outlined in the table below:

Stage:	Vulnerable to:	
	Malice	Error
Development of hardware/software	✓	✓
Storage of machines between polls	✓	
Backup copy		✓
Transport of modules	✓	
Loading of votes from modules	✓	✓
Separation of ballot papers for counting (where multiple ballots are cast on the same day)	✓	✓
Counting results	✓	✓

Figure 1: Vulnerabilities

2 Law

The introduction of e-voting raises questions about the legal position of:

- the electoral rules
- the electoral results
- the vendors of the system

It is vital that the law moves to meet the new challenges posed by introducing new technology.

¹ The number of PCs involved at this stage and the nature of their interconnection is somewhat unclear [see Section 3.2]

2.1 Electoral Rules

The Irish Electoral Act [Ele92] 1992 laid out the rules by which votes should be counted in Irish elections. The act outlined the particular form of Proportional Representation - Single Transferable Vote (PR-STV) mandated in the Irish constitution, including the specific rules to be followed during counting. Thus the Irish Electoral system was completely described in law.

Since the introduction of enabling legislation for electronic voting in 2001, the rules for deciding Irish elections are no longer dictated solely by the relevant law. The software within the system is in fact the final arbiter. Under current agreements between the Irish government and Nedap/Powervote this leads to an extraordinary situation. The count rules no longer belong to the Irish people, are no longer public and are subject to change without legal procedures.

The Electoral Law has been interpreted by the Department in a document called the "Count Rules"². This document serves as the user specification for the programmer. No other documentation exists except the application itself which is in some 150 to 200 modules of Borland Delphi code. The overall codebase is 200,000 lines of code originally established for use in the Netherlands. It has been modified for use in Germany, in Ireland and in the UK. It has recently been further modified for use in a trial in Brest, France. The reviewers' comments [NTec] indicate that there is no separation between the UK and the Irish code base for certain modules. This is a very dangerous practice since the electoral rules are completely different in the two countries - the UK uses "first past the post" whereas Ireland uses PR-STV.

2.2 Electoral Results

In the paper system, the law required that ballot papers be kept for a minimum period of six months in provision for disputes arising. In such cases, a court could require that the paper ballots be re-examined. A similar provision has been made within the electronic system, but as the only records of votes cast would be electronic, the only evidence which could be presented in court would be electronic evidence (or a printout of electronic evidence, which is of course no more reliable). It is difficult to have electronic evidence admitted in a court of law [Lam02] and rightly so, since it is so much more easily manipulated and tampered with.

The legal position of electronic ballots has not been tested in any Irish court, but the possibility that results could be successfully appealed on this basis should certainly be considered.

² Available for download from <http://evoting.cs.may.ie/Documents/DoEHLGCountRules.doc>

2.3 Vendors

Electronic voting systems are different from other software and hardware products, because of the vital role they play in the democracies where they are used. It makes sense therefore that the vendors of such products should be treated differently. The commercial interests of those companies cannot be allowed to take precedence over democratic interests.

Perhaps the most obvious conflict between these interests is in the matter of trade secrets. Normal practice within the software industry is for software developers to keep the source code for their products secret. The same applies to all the documentation produced during the development process, including design documents, and test strategies and results.

If the public is to be satisfied that the system was well developed and does what it is supposed to do, this documentation must be made publicly available, so that those with the skills to examine its quality have that opportunity. While this approach prioritises public interests over private, it is not all negative for the company. There are many successful businesses today that use the open source model. For example, the Australian electronic voting system was produced by a commercial company, and its source code is available for download [Aus]. This has already resulted in several flaws being discovered and corrected [Zet03].

A further conflict of interest is this: if there is a flaw in the system it is very much in the public interest that such a flaw be discovered and corrected. This would be bad publicity for the vendor, however. Unfortunately it is not safe to assume that a business will put the correct working of democracy ahead of its own reputation. Therefore it must be made as difficult as possible for vendors to deny or ignore flaws in the system. Again, this requires the highest level of public scrutiny.

The ownership of source code and similar materials (such as design documentation) is another important issue where standard industry practice conflicts with the best interests of the public. Usually software vendors sell licences to use pre-compiled versions of their product and retain copyright of the code itself. However, if the source code were owned by the people instead of the vendors, we would be protected from at least two extremely undesirable scenarios: the case where a vendor or vendors go out of business; and the possibility of vendor refusing to comply with the government's wishes. First, should the vendor go out of business, the future of our electronic voting system would be significantly more secure. There being no doubt as to the ownership of the code, the Government would be considerably freer in their choice of a replacement vendor. Second, since the government would be in a position to switch to a competitor, the vendor could not make unreasonable price increases or other undesirable policy changes, nor could they refuse to make alterations/updates to the software.

The contract between Nedap/Powervote and the Irish Government explicitly retains ownership of the embedded software in the voting machines for Powervote.

Clause 10.1.2 Notwithstanding the vesting of ownership of the Ordered Equipment in the Customer, the Customer and Returning Officers acknowledge that the Embedded Software remains subject to a licence granted by the Suppliers and no transfer of ownership of the Embedded Software shall occur, including but without limitation any Intellectual Property Rights in the Embedded Software. The Customer and Returning Officers acknowledge that the Embedded Software is the Confidential Information of the Suppliers.

<http://evoting.cs.may.ie/Documents/DoEHLGPowervoteNedapContract.doc>

This is a reversal of the position laid out in the original request for tenders.

Clause 8.4 All software paid for and developed to Departments specification will be the property of the Department.

<http://www.electronicvoting.ie/pdf/Req for tenders doc - June2000.doc>

The Government has had to provide an indemnity to the Commission on Electronic Voting [CEV] in case the source code it is examining falls into the hands of competitors [Cor04]. To have allowed such a situation to develop shows a significant failure on the part of the Department to set out clear expectations that it should own any software developed for elections. The cost of the software is estimated to be €467,000 for the counting system.

It is vital that these potential conflicts of interest are recognised and addressed by those introducing electronic voting. It is not good enough for a government to rely solely on the advice, opinions and information provided by vendors. These must all be scrutinised by experts with no personal or commercial interest in the system.

3 Politics

The transparency of voting in Ireland, already eroded by the technology of the system itself, is further reduced by the way in which the introduction of the system has been managed. The procurement of evoting is being overseen by a department of the presiding government. The Minister for that department is the director of elections for one of the ruling parties for the upcoming elections. A policy of secrecy is evident, with commercial sensitivity being prioritised over public need to know. This policy is clear from the difficulty faced by those requesting information on the system, as discussed below.

Such secrecy compounds a serious problem inherent in the introduction of technology in publicly sensitive areas. Public understanding of the system is necessarily reduced as the complexity increases. This is unnecessarily exacerbated by a lack of information. Even those with the knowledge to confirm or deny the public's fears and hopes for the system cannot make comment on the suitability of the system.

There is a strong case to be made that the responsibility for decisions regarding voting technology should be taken out of government hands. While this is an issue relevant to politics, it should never become a political issue. An Electoral Commission, such as exists in the UK, would reduce the risk of mixing political motives with public interest.

3.1 Computer Science Meets Politics

Computer science is a relatively new science, only 50 years old, and the public perception of it is quite different from that of other sciences. Perhaps this is influenced by the general availability of computers and their use in practically every aspect of our daily lives. Particle accelerators are not nearly as commonplace as PCs.

No bridge would be built in the developed world without the involvement of an engineer, and yet computer systems are commonly installed by people with minimal knowledge and training. This works adequately in many low-priority situations, and so it may not be obvious that high-priority systems require greater expertise. Similarly, software is generally developed in a very ad hoc manner, which results in high failure rates. Again, this is generally a frustration rather than a major problem and is therefore acceptable in most contexts.

Computer science has, in fact, discovered laws of computation as immutable as those of physics, but the peculiar position of computer science in the public perception makes it very difficult to convey such concepts. While it may sound strange to those with no computer background, computer science tells us that we can never test a computer program enough to be absolutely certain of its behaviour.

NASA, whose employees' lives depend on the reliability of its software, are among the world's most accurate software developers, and yet they provide convincing evidence of this phenomenon. They use sophisticated techniques to reduce the faults in their software to a minimum. But studies have shown that NASA could expect 60 faults to be contained in a software project the size of the Groenendaal counting software³ [Fis96].

³ The IES count-software used by the Nedap/Powervote system.

The techniques mentioned above require more resources, including time, than does ad hoc development. So they are generally used only for safety critical applications such as medical equipment and driverless trains. There is a strong argument in favour of the use of these techniques in government applications such as the penalty points system used to keep track of traffic offences in the Republic of Ireland, and in electronic voting. Failures in such systems could result in innocent people going to jail, or the wrong people getting into government.

Because of public perceptions of computer science, people without adequate training may attempt tasks that require deeper knowledge. For instance, the specification of requirements for a computer system is a vital stage that requires certain expertise. It is vital that the specification for a computer system is well thought-out and covers all the requirements for the system. Mistakes made at this stage of system development can have severe effects later in the process.

The resulting lack of consultation with computer professionals has caused many problems in many walks of life, not least in the introduction of electronic voting in Ireland. Failures at the specification stage, which could have been easily identified by computer scientists, remain within the system. The most glaring example of this is the lack of a proper audit trail (see section 1.2).

3.2 Freedom of Information

Given that the people have a constitutional "right to designate the rulers of the state"⁴ it is notable that ownership and scrutiny of the casting, collecting and counting of votes has become a secret matter. In response to this, concerned private citizens have made use of the Freedom of Information Acts (1997, 2003 [FoI97]) to obtain as much relevant information as possible.

Attempts to obtain technical details of the electronic voting system in Ireland have been hampered by the exemptions allowed in the Freedom of Information Acts. In particular, The Department of the Environment has relied on the trade secret and the commercial confidentiality exemptions to deny access to most of the documentation from Powervote/Nedap. Surprisingly there is no documentation from Groenendaal on the counting system. In their case the Department has refused to use a section of the Acts which provides that records held by a supplier of services are deemed to be held by the Department. This decision is under appeal to the Information Commissioner.

The Department in 2003 avoided their obligations under this section by virtue of the absence of a formal contract. There was a Letter of Intent in place under which some €30m of equipment and software were purchased. Yet the Department held that there was no current contract.

⁴ Bunreacht Na h'Eireann/Constitution of Ireland, Article 6.

Other factors inhibiting the public in understanding this system is a marked absence of project documentation, testing schedules and testing results. No end-to-end tests⁵ have been independently conducted other than the running of actual pilot elections in three constituencies in 2002. The available reports from this pilot exercise indicate that the normal reconciliation procedures completely failed. The Returning Officer proceeded on the basis of his own judgement that matters seemed to him to be in line with his expectation⁶.

Mr. Joe McCarthy's personal requests under the Freedom of Information legislation have cost him €2,882 to date. Every delay allowed under the Act has been used by the Department to frustrate free access to the records. In a letter received on April 23rd, the department again refused to release certain files in the possession of the vendors of the system. Under Freedom of Information legislation, citizens may request records in the possession of "a person who is or was providing a service under a contract for services". The department refused the request on the basis that:

This Department does not accept that Nedap Powervote are providing a service for the Department under a contract for services.

<http://www.evoting.cs.may.ie/Documents/DoEHLGDenialofContract.doc>

This is in direct conflict with the contract itself (referenced earlier), which in recital 1 establishes a contract for services between Nedap/Powervote and the department.

WHEREAS

1. The "Suppliers" will supply to the Department and Returning Officers (as hereinafter defined) designated by the Customer the Equipment (as hereinafter defined), including the Embedded Software (as hereinafter defined), Support, Project and Maintenance Services (as hereinafter defined) and as described in this Agreement.

<http://evoting.cs.may.ie/Documents/DoEHLGPowervoteNedapContract.doc>

3.3 History of Electronic Voting in Ireland

The introduction of electronic voting is the biggest change to the Irish electoral system since the establishment of the state over 80 years ago. The idea was introduced by the Fianna Fáil/PD government in 1999 with an Act to allow the use of actual ballot papers for research into voting methods. In 2000 a public tender was issued and it was won by the Powervote/Nedap/Groenendaal consortium.

Later in 2001 an amendment to the Electoral Act was passed allowing the Minister to approve machines for electronic voting. Remarkably, no objective or legal criteria were set for the machines or the software.

⁵ End-to-end tests are generally considered to be a vital part of the testing process [Tam02].

⁶ Paraphrased from comments made during appearances by Mr. John M. Fitzpatrick on Dublin radio station Newstalk106 and national radio station RTE1 on Friday the 16th of April.

The first enabling legislation was brought in as part of a broad, controversial bill. Debate on this bill was guillotined⁷ by the Government. Several members voiced their concerns about the system at the time⁸. They were assured that the introduction of electronic voting would not go ahead without all-party consensus.

This Government will not proceed without unanimity and general agreement among the Members here.

- Minister Molloy, Seanad (The Irish Senate), 2001 June 14

The system was then used in three constituencies in the June 2002 General Election. The Government said the trial was successful, but others - including the authors - have grave reservations. The formal reports from the Returning Officers indicate many faults occurred [Fit02]. The results were declared without any external audit of the votes. Without further consultation, either with the Opposition or with the public, the Government decided in October 2002 to implement the system countrywide for the June 2004 local and European elections.

In 2003 a series of reports [Mcg03, Mcc03] were published questioning the integrity of the system and the process used to introduce it. A Parliamentary committee examined the matter but on December 18th 2003 the government parties applied the whip to close the debate just after the authors raised many technical questions. A publicity campaign was launched by the Government in February 2004 costing some €5m.

Public outcry continued to the extent that the Government has now appointed an ad-hoc Commission on Electronic Voting [CEV] to report on the secrecy and accuracy of the system. These terms of reference are narrow and do not allow the Commission to examine the integrity, cost or benefit of the system.

As we write, the Government is intent on pressing ahead in the face of the combined Opposition and with diminishing public support for the initiative.

4 Conclusion

Transparency is an integral part of the security of voting systems. It is vital that technology is not allowed to erode that transparency. Not only must the technology itself implement measures to ensure that it is trustworthy - which, in the current technological climate, means voter verified paper ballots - but the system must be managed in a transparent, non-partisan way.

Where democratic concerns conflict with commercial concerns - as in the case where publication of technical details may threaten intellectual property rights - the democratic concerns must be given priority. After all, businesses can move into other markets. We have only one democracy.

⁷ This refers to a process whereby a fixed time is set for concluding debate in the Dáil. There is no further discussion at that point, the question is put to the house and voted through by Government majority against the wishes of the Opposition. It is effectively a forced change of the law by the Government.

⁸ See Adrian Colley's summary of Dáil and Seanad debates on the subject of electronic voting - <http://www.iol.ie/~aecolley/record.html>

References

- [Aus] Australian electronic voting and counting source code.
<http://www.elections.act.gov.au/Elecvote.html>
- [CEV] The webpage of the ad hoc Commission on Electronic Voting: <http://www.cev.ie/>
- [Cha04] David Chaum. Secret-ballot receipts: True voter-verifiable elections. In *IEEE Security & Privacy (Vol. 2, No. 1)*, pages 38–47, January-February 2004.
- [Cor04] Mark Brennock Chief Political Correspondent. Last-minute indemnity for e-voting commission agreed. *The Irish Times*, April 2004.
- [Ele23] Electoral Act, 1923. Available online at the website of the office of the Attorney General http://www.irishstatutebook.ie/1923_12.html.
- [Fis96] Charles Fishman. They write the right stuff. *FastCompany*, 06, Dec 1996.
<http://www.fastcompany.com/online/06/writestuff.html>
- [Fit02] John M. Fitzpatrick. Dublin county post election report, June 2002.
<http://evoting.cs.may.ie/Documents/PostElectJune2002.pdf>
- [FoI97] Freedom of Information Act, 1997. Available online at the website of the office of the Attorney General http://www.irishstatutebook.ie/1997_13.html.
- [JRB03] Andreu Riera Jorba, Jos Antonio Ortega Ruiz, and Paul Brown. Advanced security to enable trustworthy electronic voting. In *Proceedings of the 3rd European conference on e-Government*, pages 377–384, 2003.
http://www.scytl.com/docs/ECEG2003_full_paper.pdf
- [Lam02] Paul Lambert. Who has their eye on your online activities? *The Sunday Business Post*, May 2002. <http://archives.tcm.ie/businesspost/2002/05/05/story319171.asp>
- [McC03] Joe McCarthy. Report on the IES Counting Software.
http://www.evoting.cs.may.ie/Documents/report_oniescountingsoftware.pdf
- [McG03] Margaret McGaley, J. Paul Gibson. Electronic Voting: A Safety Critical System.
<http://www.evoting.cs.may.ie/Project/report.pdf>
- [Mer92] Rebecca T. Mercuri. Physical verifiability of computer systems. In *5th International Computer Virus and Security Conference*, March 1992.
- [Mer02] Dr. Rebecca Mercuri. A better ballot box? *IEEE Spectrum Online*, October 2002.
- [NTec] Nathean Technologies. Code review of ies build 0111 for the department of the environment, heritage and local government - page 25.
http://www.electronicvoting.ie/pdf/Nathean_Code_Review_Dec03.pdf
- [Sch00] Bruce Schneier. Voting and Technology. *Crypto-Gram*, 00(12), Dec 2000.
<http://www.schneier.com/crypto-gram-0012.html - 1>
- [Soc04] Irish Computer Society. The ICS calls for audit trail in e-voting system, Mar 2004.
<http://www.ics.ie/article-027.shtml>.
- [Tam02] Louise Tamres. *Introducing Software Testing*. Addison-Wesley, 2002.
- [U.S] U.S. Public Policy Committee of the Association for Computing Machinery. E-voting technology and standards. WWW page.
<http://www.acm.org/usacm/Issues/EVoting.htm>.
- [Zet03] Kim Zetter. Aussies do it right: E-voting. *Wired News*, 2003.
<http://www.wired.com/news/ebiz/0,1272,61045,00.html>

