

[CLICK HERE FOR DEMOCRACY:](#)

# A comparative analysis of electronic elections conducted between 2000–2005

Alun Thomas

Project Leader

23 May 2007



# Table of Contents

Executive Summary .....	7
Web Addresses.....	13
Chapter One: Arguments on electronic voting .....	15
Internet voting – arguments against.....	16
Direct Recording Equipment (DRE).....	17
Chapter Two: The American experience: DRE .....	23
Ohio.....	26
Florida.....	28
Missouri .....	30
Chapter Three: The Estonian Experience: Internet Voting.....	35
Contextual information .....	36
E-voting project .....	37
The election results and management process .....	40
Critique .....	41
Chapter Four: The Indian Experience: EVM.....	43
The Indian Electronic Voting Machine (EVM).....	44
How the system fared.....	45
Chapter Five: The United Kingdom Experience: Multiple Voting Channels.....	49
Background.....	49
Case Study: The City of Salford .....	50
Background .....	50
Preparation .....	51
The voting process .....	51
Counting of Votes .....	52
Participation .....	52
The 2002 pilot schemes .....	54
Case Study: Crewe and Nantwich Borough Council.....	55
Summary .....	56
The 2003 pilot schemes .....	58
Case Study: St Albans City and District Council .....	60
Voting period .....	61
Security and Authentication.....	61
Elector feedback.....	61
Logistical and support issues concerning polling stations.....	62
Issues with touch screen kiosk voting at polling stations .....	62
Issues with the online electronic register at polling stations.....	63
Issues with internet browser requirements.....	63
Impact on turnout.....	63
Chapter Six: The Australian Experience: EVACS .....	65
Background to EVACS and the 2001 trial.....	65
Testing and auditing of EVACS .....	65
The electronic voting system .....	66
Security .....	66
Casting a ballot .....	67
How the system fared.....	68
Pre-polling Centres .....	68
Electronic voting on polling day.....	69
From the electors’ perspective .....	70
The elimination of unintentional voting errors .....	71
Informal voting .....	71

Chapter Seven: Concluding Remarks .....	73
Appendices.....	75
Appendix One: Matrix of Voting Technologies by Criterion.....	75
Appendix Two: Salford pilot scheme debriefing session, 11 May 2000.....	89
Bibliography .....	91

## Table of Tables

Table 1: US Election Year 2004 Reported Incidents.....	24
Table 2: Overview of reported incidents in the US 2004 election.....	33
Table 3: Estonian computer usage by age group .....	35
Table 4: e-voting Statistics Estonian Municipal elections 2005 .....	41
Table 5: General Election 2004 India .....	43
Table 6: Summary of 2000 Local Government Election Pilot Schemes .....	50
Table 7: Irlam ward 2000 election turnout .....	52
Table 8: City of Salford 2000 electronic voting pilot questionnaire responses .....	53
Table 9: Multi-channel pilot schemes turnout .....	57
Table 10: Post voting questionnaire results summary .....	62
Table 11: St Albans election turnout 2000–2003 .....	63
Table 12: Breakdown of the different channels used in the St Albans 2003.....	64
Table 13: Electors perspective on EVACS .....	70
Table 14: Voting errors recorded in 2001 and 2004 state general elections.....	71

## Table of Lists and Figures

Chart 1: US Election Year 2004 Reported Incidents .....	25
Chart 2 US Election Year 2004 Reported Incidents, Ohio. ....	28
Chart 3: US Election Year 2004 Reported Incidents, Florida .....	30
Chart 4: US Election Year 2004 Reported Incidents, Missouri.....	32
Diagram 1: General description of e-voting and the envelope method. ....	37
Diagram 2: Estonian e-voting and system architecture .....	39
Diagram 3: India’s Electronic Voting Machine.....	44
Chart 5: Internet and telephone voting volumes St Albans 2003 pilot .....	64

## Executive Summary

This paper provides a broad overview of the issues associated with 'Electronic Voting Systems' (EVS) specifically, security and vulnerability of the technology, and examines whether or not the use of such technology has resulted in acts of electoral fraud, or has threatened the legitimacy of democratic processes, as opposed to implementation or ICT deficiencies. EVS is a descriptive term that covers a wide range of technologies developed or adapted to assist individuals in casting a vote. They include, among others, Direct Recording Equipment, a kind of electronic ballot box; and the Internet which can be utilised as a ballot transmission tool. The research is based on a 'desktop' analysis of reports and commentary produced on actual electronic elections; with the central aim of establishing whether the assumptions regarding electronic voting made by academics, technology experts, election officials and other interested parties came to fruition.

The paper examines electronically assisted elections conducted in five discrete jurisdictions to ascertain how they functioned in practice and is divided into six parts, covering the key arguments on electronic voting and case studies of electronic elections in the US, Estonia, India, United Kingdom (UK) and to a limited extent, Australia.

Chapter one is based around the arguments raised in relation to the adoption of EVS to facilitate elections and draws on commentary stemming largely from the US for two key reasons. The US has been using mechanical and electronic voting equipment since the 1970s resulting in the development of a knowledge bank. Further, the closeness of the 2000 presidential election, exasperated by the failure of older mechanical ballot marking devices, ignited interest and debate in alternative voting technologies.

Proponents of EVS argue that they improve access and convenience for voters; they can provide linguistic support and translate languages, and display elector's choices on a single screen for verification prior to vote casting. EVS are held to mitigate the problem of over and under voting, or informal voting, and are thought to address early problems associated with ballot marking devices, specifically the potential ambiguity regarding an elector's intention. Perhaps the most important aspect of EVS is their ability to be configured to assist people with visual or physical impairment, followed closely by their ability to allow electors in remote areas to participate in an electoral event without the need to travel great distances.

The main areas for concern evolve around the security and integrity of the software and operating systems used to facilitate electronic voting, in particular, concerns that software manufacturers' and/or election officials may fraudulently conspire to manipulate or distort results. A further concern is raised regarding electoral entitlements and whether or not it is possible for people who are not entitled to vote do, and that electors might vote more than once.

What becomes apparent from the discussion is that the concept of EVS is a challenging one, with many competing views for and against the widespread adoption of such technologies. The concerns raised may be real and valid but at the same time

not insurmountable. What is considered important is not the construction of an infallible system, but one which monitors the processes and, should the need arise, procedures to resolve any issues.

Consideration should also be given to the changing dynamics of society, be they cultural, technological or social, and where applicable amend contemporary structures and processes, and old mind sets, to reflect these changes, including the adoption on new technologies to assist with the facilitation of elections.

Chapter two contains a more in-depth analysis of the American experience in relation to EVS. Electronic voting in three US States during the 2004 presidential election are evaluated: Ohio; Florida; and Missouri. This approach provided an opportunity to test perceived vulnerabilities against actual election experiences. Collectively the three states offer an insight into the US electoral process which used various EVS, most commonly 'Direct Recording Equipment' (DRE) and Optical Scanning Machines (OSM)<sup>1</sup>.

The observations from the three states evaluated are quite intuitive. Whilst there is a raging debate on the merits of using EVS, including many well documented failures, what becomes apparent is that the risks discussed in chapter one do not appear to have eventuated. Although critics are concerned EVS offer the potential for collusion between equipment manufacturers and election officials to manipulate results, or that hackers could break into DRE and cast multiple votes or erase previous ones, there appears to be no actual cases of such incidents occurring.

A more pressing concern for the American people and electoral officials is the number of general procedural problems associated with their electoral systems, as reported by actual electors, as opposed to the implementation of new voting technologies.

The analysis of electoral complaints generated during the 2004 Presidential election, and compiled by Non Government Organisations, paint a picture of a US wide electoral system that is straining under the weight of poor administration and electoral practice.

Chapter three discusses Estonia, a parliamentary democracy which conducted a country wide Internet voting trial in October 2005. Estonia was chosen for a case study due to their decision to offer Remote Internet Voting (RIV) to all eligible electors. This trial provided an opportunity to test perceived security threats or impediments to adopting the Internet to facilitate elections in a real electoral event.

An encouraging aspect for proponents of EVS is that Estonia overcame the issue of security, which is considered the biggest hurdle associated with the use of the Internet for the purpose of casting votes. This was achieved through the use of 'digital signatures', 'public key cryptography' and 'digital encryption'. These electronic security measures have been held by some commentators as an acceptable means to protect both the identity of the elector and the integrity of the electoral system.

---

<sup>1</sup> An OSM is used to count completed ballot papers. Typically an elector marks the ballot paper in a predetermined spot corresponding to their preferred candidate; completed ballots are then fed into the OSM which counts the marked ballots.

Although the Estonian trial can be considered a success from the point of security robustness with no reported incidents of electoral fraud, it should be noted the trial was conducted in unique circumstances. In Estonia, since 2002, it has become mandatory for all residents to obtain an electronic identification (ID) card. Since its inception the card has become an integral part of Estonian life, and is linked to a range of e-services, including the identification systems of private banks and was an essential element of the trial.

The security measures afforded by the use of electronic ID cards in Estonia can be considered a positive. However, such a method could prove problematic for other democracies, in particular in a country such as Australia where there has been a tradition of opposition to such propositions. Interestingly, the Australian federal government is considering the introduction of an 'Access Card' as a means to streamline the delivery of government services, namely health and social security benefits, and may be in the future the same card could be used to facilitate secure electronic voting.

Chapter four provides an overview of the 2004 General Election held in India, the world's largest democracy, which conducted the first country-wide election using 'Electronic Voting Machines' (EVM).

Like many democracies, India is striving to modernise and streamline its voting system through the adoption of electronic technology. The approach adopted in India was to develop a system that was simple to use, understand, and not reliant on sophisticated architecture or software. The simplicity of the EVM is considered by some to be its strength as it does not include copious amounts of software code, and as such reduces avenues for hackers to embed malicious election distorting viruses.

India can be considered a quiet achiever in the realm of electronic election modernisation. Its experiment resulted in approximately 380 million electors, 56 per cent of eligible voters, casting a vote on one of the 1 million plus voting machines in the world's largest experiment in electronic voting to date, whilst the process was not perfect, it can be considered a success.

Chapter five discusses the UK modernisation of electoral processes that commenced in earnest in 2000. The case studies examined in this chapter cover local government authorities, which conducted electronic voting pilots over three years. The UK pilots are of particular interest as they trialled numerous methods/channels, including digital television, touch-tone telephony, SMS text, DRE and the Internet.

Local authorities were required to produce evaluation reports after each trial. The assessment criteria for these reports were initially stipulated by the Home Office and then later by the UK Electoral Commission. The evaluation reports were quite detailed, but the aspects of interest in regard to this paper are the discussions around fraud.

In the UK electronic trials there were no examples of fraud discovered. The UK government was especially keen to build public trust in the trials and it stipulated that it was made mandatory for all alleged incidences of fraud to be acted upon. One proven incidence of electoral fraud during the trial period was not related to electronic

voting. Other incidences, although not fraudulent, involved some electors mistakenly attempting to vote twice.

Chapter six discusses Australia's contribution in the field of electronic voting. Australia has been slow in developing electronic voting systems, although computers have been a fundamental part of the electoral system for many years; in particular, the management of electoral rolls, counting of ballots, and distributing preferences. This chapter focuses on the ACT Legislative Assembly Elections of 2001 and 2004, where an 'Electronic Voting and Counting System' (EVACS) was developed and utilised.

The catalyst for the ACT trial stems back to the 1998 Legislative Assembly Election, where a close result in the Molonglo electorate necessitated a recount. Two candidates were separated by three votes and a recount revealed an error in the initial manual counting process, resulting in calls for an automated system to increase the speed and accuracy of the election system.

Perhaps the most encouraging aspect of EVACS is the potential to eliminate unintentional voting errors through automatic numbering of candidates as they are selected by an elector. Once an elector makes their first candidate choice the computer program automatically marks that preference as one (1) in the candidate square and subsequent choices are marked sequentially thereafter until all choices are exhausted.

In addition a matrix has been developed as a tool to assist in the understanding of the strengths and weaknesses associated with different electronic voting methods. The matrix includes a set of benchmark criterion for assessment purposes and has been applied to contemporary and evolving electronic voting methods (refer appendix 1).

## Abbreviations

AHTSF	Ad Hoc Touch Screen Task Force
AEA	Association of Electoral Administrators
BEL	Bharat Electronics Limited
CESG	Communications-Electronics Security Group
CD	Compact Disc
DRE	Direct Recording Equipment
CPS	Crown Prosecution Service
ECI	Election Commission of India
ECIL	Electronic Corporation of India Limited
e-ID	Electronic Identity Card
EIRS	Election Incident Reporting System
EPC	Election Protection Coalition
EVACS	Electronic Voting And Counting System
EVM	Electronic Voting Machine
EVS	Electronic Voting Systems
FEC	Federal Election Commission
FEI	Fair Election International
HAVA	Help America Vote Act 2002
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IPI	Internet Policy Institute
IT	Information Technology
ICT	Information Communication Technology
LGA	Local Government Association
NASED	National Association of State Election Directors
NSF	National Science Foundation
OASIS	Organization for the Advancement of Structured Information Standards
OSM	Optical Scanning Machine
PPERA	Political Parties, Elections and Referendums ACT 2000
PKI	Public Key Infrastructure
PC	Personal Computer
PIN	Personal Identification Number
RIV	Remote Internet Voting
SAIC	Science Applications International Corporation
SOLACE	Society of Local Authority Chief Executives
UK	United Kingdom
US	United States
VCA	Vote Counting Application
VVF	Verified Voting Foundation
VFS	Vote Forwarding Server
VSS	Vote Storage Server
VVPAT	Voter Verified Paper Audit Trail
WAEC	Western Australian Electoral Commission

## Web Addresses

British Broadcasting Company (BBC) Online	<a href="http://www.bbc.co.uk/">www.bbc.co.uk/</a>
Californian Secretary of State	<a href="http://www.ss.ca.gov">www.ss.ca.gov</a>
Congressional Research Service (US Dept of State)	<a href="http://fpc.state.gov/c4564.htm">fpc.state.gov/c4564.htm</a>
Diebold Election Systems	<a href="http://www2.diebold.com">www2.diebold.com</a>
Election Commission of India	<a href="http://www.eci.gov.in">www.eci.gov.in</a>
Estonian National Electoral Committee	<a href="http://www.vvk.ee/engindex.html">www.vvk.ee/engindex.html</a>
European Commission	<a href="http://ec.europa.eu/index_en.htm">ec.europa.eu/index_en.htm</a>
Fair Election International	<a href="http://www.fairelection.us">www.fairelection.us</a>
IDABC European eGovernment services	<a href="http://ec.europa.eu/idabc/en/home">ec.europa.eu/idabc/en/home</a>
The Internet Policy Institute	<a href="http://www.internetpolicy.org">www.internetpolicy.org</a>
The National Science Foundation	<a href="http://www.nsf.gov">www.nsf.gov</a>
The UK Electoral Commission	<a href="http://www.electoralcommission.org.uk/">www.electoralcommission.org.uk/</a>
The University of California, Berkeley	<a href="http://www.berkeley.edu/">www.berkeley.edu/</a>
The US Federal Election Commission	<a href="http://www.fec.gov">www.fec.gov</a>
The Western Australian Electoral Commission	<a href="http://www.waec.wa.gov.au">www.waec.wa.gov.au</a>

## Chapter One: Arguments on electronic voting

Electronic voting systems (EVS), including Direct Recording Equipment (DRE) are an element of the modernisation process of electoral reform that have been used since the 1970s, in particular in the United States (US). Typically DRE consists of a screen similar to an 'automatic teller machine', whereby electors cast their vote by touching the screen. Internet voting is an extension of DRE and features next generation software and hardware configurations, and differs most from DRE in that it allows for the casting of ballots online. DRE are typically located at polling places. For the purpose of this paper these kind of electronic voting technologies are grouped under the collective term, EVS. Although EVS are considered by some to be the most versatile and user friendly form of voter technology available they have a considerable public relations challenge to overcome before widespread public confidence in the concept is achieved.

This paper intends to inform the reader on some of the strengths and weaknesses associated with their use. The paper has not been written from a technological perspective, nor does it adopt a forensic analysis of information and communication technology (ICT) systems. Such analysis has been conducted by various academics and institutions with expertise in this field, some of which has been included in this paper.

The mechanisation of electoral systems has developed according to the technological advances of a given era. The latest, EVS, present a new avenue to conduct elections and has resulted in a lively debate amongst those with an interest in both democratic processes and technological innovation. Pilot programs in a number of countries have thrown up a range of issues for debate, which will be examined in this chapter.

The key arguments raised in favour of EVS include improved access for voters and convenience. Other purported benefits are their capacity to translate a multitude of languages, display elector's choices on a single screen for verification prior to vote casting, and the fact that they can be configured to assist people with visual or physical impairment. They can mitigate the problem of over and under voting, or as it's known in Australia informal voting, and are held to address early problems associated with ballot marking devices,<sup>2</sup> specifically the potential ambiguity regarding an elector's intention.

The main areas for concern evolve around security and integrity. There is concern that software and operating systems can be manipulated to distort results, that people who are not entitled to vote might do so, and that others might vote more than once.

---

<sup>2</sup> For example the mechanical lever machines that produced the now infamous 'hanging chads' of the 2000 US election.

This chapter focuses on two platforms currently the subject of academic and policy debate, the Internet and DRE.

## Internet voting – arguments against

### Security

Perceived impediments to the introduction of Internet voting include system or communication failures and issues related to elector privacy, and the accuracy and robustness of elector verification processes. Communication or system failures are incidents or events that could disrupt or stop the election process and include:

- ‘Jamming’, where a hacker overloads a website thus disabling communication;
- ‘Man in the middle’ attacks, where a hacker produces an identical or impostor web site, essentially to steal personal information;
- ‘Page jacking’, where a user has difficulty accessing a desired web site and is constantly redirected to an impostor site; and the more benign
- ‘Bottlenecks’, where information requests and traffic volume retard access to other users.<sup>3</sup>

Critics have highlighted the limitations and vulnerability of home computers, or the ‘platform’ electors use to engage in Internet elections. These platforms are believed to be vulnerable to the threat of ‘malicious payloads’ such as those outlined above, and the pervasive nature of their ‘delivery mechanism’.<sup>4</sup> ‘Malicious payloads’, or ‘attack programs’, are more commonly known as computer viruses. Viruses are disruptive and difficult to detect, especially for the average home computer user.<sup>5</sup> There is concern that hackers can exploit security holes in the most commonly used operating systems, two examples cited being the ‘Mellisa’ virus and the ‘Love Bug’.

The 1998 ‘Mellisa’ virus was one of the first widespread email delivered viruses, infecting over a million PCs globally. Mellisa was followed in 2000 by the ‘Love Bug’, which was programmed to delete computer files and to raid email applications for the purpose of multiplying by sending itself to other computers contained in people’s electronic address book.

### Privacy concerns

Closely linked to issues of security are concerns relating to privacy. Opponents of Internet voting contend that electors should be able to cast a vote in the confidence that it has not been subject to tampering. There is apprehension that hackers may change an elector’s vote prior to authentication and encryption being applied.<sup>6</sup> However, evidence of such occurrences is sparse and any concerns are apparently pre-emptory.

---

<sup>3</sup> Elliot n.d., p.4; & Gibson 2001, pp.4-7.

<sup>4</sup> Gibson 2001, pp.4-7; IPI 2001, p.13; & Rubin 2002, p.2.

<sup>5</sup> For a more detailed analysis of such threats refer to Rubin (2002) who illustrates the point by discussing a product called ‘Backorifice 2000’ (B02K), a legitimate and freely available piece of software. The product is fully open source and runs in stealth mode, is difficult to detect and does not appear in the ‘Task Menu’ of running processes. Furthermore, its ‘open source code’ allows a hacker(s) to modify the code and recompile it as necessary to evade detection by anti-virus software. Once a computer becomes affected by a ‘malicious payload’ such as B02K, a hacker could potentially view and control the computer from a remote location.

<sup>6</sup> Gibson 2001, pp.4-7; Kohno et al. 2003; & Rubin 2002, p.2.

Perhaps more serious is the potential for coercion and electoral fraud should elections be conducted away from the supervision of officials at polling places. These concerns highlight a need for electronic systems to incorporate a verification method to establish identity to ensure a single vote.<sup>7</sup> This concern has also been raised in relation to postal voting and to date, at least in Australia, does not appear to have eventuated.

These issues are not insurmountable, with 'digital signature' technology thought to be one solution in terms of verification. Digital signatures provide an authentication method and a means to protect privacy. There are, however, potential barriers to the adoption of digital signatures as they are expensive, and represent a significant cost and access factor.<sup>8</sup>

### **Standards**

The adoption of Internet voting, in particular in the US, would require strengthening of the current testing regimes for voting systems, namely those associated with DRE. In the US, where DRE is actively utilised, such systems and software are periodically reviewed against the Federal Election Commission's (FEC) guidelines for voting systems. Current standards do not yet contain any reference to Internet voting, and as such the relevant guidelines would require amendment.

It is considered that the advent of Internet voting necessitates the creation of a sub set of new standards, for example software review benchmarks, platform review standards, standards for security systems and logic testing. In addition, a move to Internet voting on a wide scale may necessitate legislative change to criminalise coercive or fraudulent behaviours, including invasion of privacy.<sup>9</sup>

### **Direct Recording Equipment (DRE)**

DREs are best described as touch-screen terminals and are typically located at polling places. It has been suggested that the controversy surrounding the 2000 presidential election in the United States, 'famously determined by just 537 votes in Florida and one Supreme Court decision'<sup>10</sup>, was the catalyst for the introduction of new voting technologies.

DRE is intended to resolve the issues experienced in 2000 by providing a more timely and accurate count. Critics caution that these new technologies are not widely tested and may also result in lost or miscounted votes. There is further concern that the software may be manipulated to commit election fraud, and unlike conventional systems, lack a paper audit trail.<sup>11</sup> Federal funding and the *Help America Vote Act 2002* (HAVA) are expected to provide US electors with the framework to support new technologies in future elections.

### **Residual vote**

The accuracy of voting systems is often calculated by the size of the 'residual' or 'lost vote'. That is, the difference between the number of electors who attended a polling

---

<sup>7</sup> Elliot n.d., p.4; Gibson 2001, pp.4-7; IPI 2001, pp.1-2; & Rubin 2002, pp.2-3.

<sup>8</sup> Elliot n.d., p.4.

<sup>9</sup> *Ibid*, pp.4-5.

<sup>10</sup> Reich & Biever 2004, p.6.

<sup>11</sup> Reich & Biever 2004; & Kohno et al. 2003

place and the number of actual votes allocated to candidates.<sup>12</sup> Optical scanning machines are considered the most accurate, with a residual vote of 2.1 per cent, compared to punch card machines at 2.9 per cent, and DRE at 3 per cent. The high residual vote associated with DRE has been linked to their design, which requires electors to navigate through complicated screens, resulting in some people failing to complete the process and vote effectively.<sup>13</sup>

A more recent study into residual votes revealed that the introduction of DRE in Florida has reduced the number of lost votes caused by over-voting. Over-voting, like informal voting in Australia, is a descriptive term for incorrectly completed ballots and essentially means an elector made too many marks (preferences) on the ballot. Conversely, under-voting means an elector made insufficient marks on the ballot. The reduction in lost votes is believed to be a result of the *Florida Election Reform Act 2001* that prescribes the conditions for conducting elections and importantly, requires DRE to disallow over-voting. The 2002 Florida primary election, the first occasion that DRE was widely used in that State, was considered a success in regard to reducing the levels of under and over-votes when compared to 2000 levels. A 40 per cent reduction in residual votes was recorded in 2002, from 3.1 per cent to 1.8 per cent, and in the 2004 Presidential election, an ‘historical low’ 0.4116 per cent residual vote rate was recorded, compared to 2.93 per cent in 2000.<sup>14</sup>

Apart from the residual vote, acceptance of a particular voting system depends on the perception of fraud and security. There is a growing concern that touch screen voting machines may allocate votes to the wrong candidate or be used to facilitate election fraud.<sup>15</sup> It is in part due to these concerns that criticism against new voting technologies has gained traction.

In 2002, a local government election in New Mexico, using DRE technology, was called into doubt when the system registered only 36,000 out of the 48,000 votes cast. Investigations revealed that the discrepancy occurred when the votes were downloaded from the voting machine’s memory cards to a central tabulator. A bug in the software had directed the tabulator to ignore votes past a certain threshold. The software manufacturer located and resolved the problem, and the lost votes were located and retrieved from the backup memory of the individual voting machines.<sup>16</sup>

Herein lies a key issue for opponents of electronic voting technology; that software technicians rather than election officials are called upon to address electoral/and or administrative problems and that democratic processes will perhaps become beholden to technocratic administrators. The counter argument for proponents of such technology holds that the case outlined above suggests the system works well, because a high level of residual votes were noticed by election officials, the system discrepancy found, and the ‘lost votes’ retrieved.

It should be noted that computers are already widely used in electoral systems for the purpose of managing electoral rolls and for conducting complex preference counts

---

<sup>12</sup> The residual vote can be used to calculate the accuracy of paper, mechanical or electronic voting systems.

<sup>13</sup> Reich & Biever 2004.

<sup>14</sup> Jones 2006, pp.127, 128, 134.

<sup>15</sup> Reich & Biever 2004.

<sup>16</sup> *ibid.*

and distributions, and that the use of sophisticated technology already requires maintenance to be conducted by experienced technical professionals, but do not appear to generate such suspicion.

### **American concerns**

In direct response to concerns raised in relation to security of DRE voting equipment, the then Californian Secretary of State, Kevin Shelly, established the 'Ad Hoc Touch Screen Task Force' (AHTSTF) in February 2003. The taskforce was made aware of concerns in relation to the security of DRE, in particular the proprietary nature of the software<sup>17</sup> which precludes public access, scrutiny and verifiability. It was assumed that the proprietary nature of the software creates an environment for potential unknown reliability and security risks.<sup>18</sup> Essentially the concerns evolve around two general themes, malicious codes embedded in the software that could affect or change votes, and the lack of 'voter verified paper audit trails' (VVPAT).

In relation to computer security, or the integrity of the DRE software, the taskforce agreed that while viruses are theoretically possible, the likelihood of such a malicious attack going undetected by federal, state and local independent testing authorities is minimal. The taskforce acknowledged some members rated such a threat as high whilst others asserted a very low possibility. There was consensus, however, that there are no proven instances of such malicious attacks or acts of fraud over the period under which DRE voting equipment has been in use. Nevertheless, the taskforce recommended the current testing and verification process be substantially improved to enhance security.<sup>19</sup>

### **Audit trail**

Transparency of process is a key element in legitimate electoral systems. Election and computer scientists contend that election results need to be verifiable to independent observers, but in the case of DRE there is no tangible (paper) evidence that votes are recorded in line with an elector's intention. In the US, the HAVA requires each voting system to produce a paper audit record. It is not clear however, about the type of paper audit trail that would be most suitable. Consequently, there are competing methodologies, ranging from whether the DRE should print out a receipt the moment a ballot is cast, or whether at the end of the polling period the DRE should print out an aggregate of all ballots cast.<sup>20</sup>

In an effort to resolve this, there have been calls to combine electronic voting with traditional paper audit trails printed and verified by the elector at the time of voting. However, an experiment of this kind in Connecticut resulted in confusion and a protracted process where electors were unsure what to do with the receipt, and voting took twice as long.<sup>21</sup>

---

<sup>17</sup> Proprietary software is software that has restrictions on using and copying it, usually enforced by a proprietor. The prevention of use, copying, or modification can be achieved by legal or technical means. Technical means include releasing machine-readable binaries only, and withholding the human-readable source code. Legal means can involve software licensing, copyright and patent law. The monopoly provided by proprietary software allows a distributor of commercial copies to charge any price for those copies (Definition sourced from [http://en.wikipedia.org/wiki/Proprietary\\_software](http://en.wikipedia.org/wiki/Proprietary_software)).

<sup>18</sup> AHTSTF 2003, p.4.

<sup>19</sup> *ibid*, pp.18-20.

<sup>20</sup> Congressional Research Service 2003, p.28.

<sup>21</sup> Santosus, 2004.

The Californian AHTSTF could not reach consensus on this issue, but did acknowledge strong support for VVPAT to guard against malicious codes distorting ballots or the electoral process. It was also considered that VVPAT should be an option for local jurisdictions to choose if the DRE used is compatible. Alternatively, printouts of all ballots cast should be undertaken after the close of polls, and the process should be open to public scrutiny.<sup>22</sup>

One of the most prominent critiques of DRE was delivered by computer scientists from John Hopkins and Rice Universities, in a July 2003 paper commonly referred to as the 'Hopkins Report'.<sup>23</sup> The Hopkins Report analysed the software used in a DRE developed by a major voting system vendor in the US, and argued such systems have inadequate security provisions and are unsuitable for use in general elections.

The Hopkins Report revealed several problems, ranging from 'unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes'.<sup>24</sup> In addition, it is asserted that systems can be manipulated by voters who are able to cast multiple votes without being detected by the DRE software system, and that poll workers can (provided they have the necessary technological knowledge) modify and/or link votes to voters in a breach of privacy.<sup>25</sup>

It should be noted that the research team only 'inspected unencrypted source code, focusing on AccuVote-TS version 4',<sup>26</sup> and that the manufacturer strenuously refutes their assumptions, arguing that they 'could not occur within an actual electoral process due to the checks and balances within the equipment and those found in accepted election procedures'.<sup>27</sup> The following commentary draws upon some of the critiques raised in the 'Hopkins Report' and the rebuttals provided by the system manufacturer, Diebold.

#### **Unauthorized privilege escalation:**

The Hopkins Report asserts that voters could create their own 'homebrew' smartcards and use them in an election to cast multiple votes without leaving a trace, and that voters could use these cards to access administrative functions, i.e. view partial election results or terminate an election early. In addition, a 'malevolent poll worker' or even cleaning staff that have access to the equipment prior to an election could perform similar modifications.<sup>28</sup>

The manufacturer acknowledged the concerns raised in the Hopkins Report but maintained that those examples would require a conspiracy of such magnitude that it would have the potential to undermine any voting system. Additionally, Diebold contends that although commercial vendors supply smartcards which can be programmed by the user, they are purchased from a single vendor with a distinct

---

<sup>22</sup> AHTSTF 2003, pp.37-42.

<sup>23</sup> Kohno et al. 2003

<sup>24</sup> *ibid*, p.1.

<sup>25</sup> *ibid*.

<sup>26</sup> *ibid*, p.4.

<sup>27</sup> Diebold 2003, p.1.

<sup>28</sup> Kohno et al. 2003, p.4.

configuration to minimise risk. It is suggested that any would-be fraudster would need to know and request the same configuration without raising suspicion.<sup>29</sup>

#### **Vulnerabilities to network threats:**

The Hopkins Report discussed the vulnerability of the system posed by insecure network communication and asserted that the protocols used during the transmission of information ‘do not use cryptographic techniques’ to safeguard the data whilst in transmission or to authenticate and clarify who is the sender or receiver.<sup>30</sup> It was suggested that if information is transmitted over insecure telephone lines or wireless connections even unsophisticated attackers could perform ‘man in the middle attacks’.

Diebold countered this argument, stating that their systems are preloaded with the relevant election information prior to despatch to a polling place, then transmitted over private, disconnected networks. Furthermore, during an election the system operates ‘offline’ and when ‘unofficial election results’ are transmitted to a central location for tabulation, it is conducted over a private point-to-point network and not over the relatively ‘insecure’ Internet or dial-up Internet service.<sup>31</sup>

#### **Incorrect use of cryptography and poor software development processes:**

Upon evaluating the source code, cryptographic techniques and the quality of the software construction, the Hopkins team concluded that neither provided any confidence of the ‘system’s correctness’. In addition, it is suggested that when cryptography was used, it was used incorrectly, and that there was no evidence of disciplined software engineering processes.<sup>32</sup>

The manufacturers denied these claims, suggesting they were unsubstantiated and made without a clear understanding of election systems, and that the software examined by the Hopkins research team was an old version. Diebold contend that the assumption that there is a correct use of cryptography is not accurate, as there is no single correct means. In relation to engineering processes, Diebold assert that disciplined and professional procedures were adhered to and that is evident from engineers’ logs that highlighted areas of concern for future action.<sup>33</sup>

In light of these revelations, and no doubt in trepidation of the then pending March 2004 Primary, the State of Maryland commissioned RABA Technologies to perform an independent audit of their Diebold voting equipment. As part of the process RABA Technologies reviewed the Hopkins Report and an earlier report commissioned by the State of Maryland by Science Applications International Corporation (SAIC) who performed a risk assessment of the Diebold AccuVote-TS voting system.

In summary, the RABA report stated that the Hopkins Report and the SAIC analysis ‘were undertaken with less than the full knowledge of the *technical, operational, and procedural* components that must be considered together in assessing any voting system’.<sup>34</sup> Furthermore, RABA Technologies contend that neither of the reports adopted the concept of ‘defense (sic) in depth’ in their analysis. In other words,

---

<sup>29</sup> Diebold 2003, p.3.

<sup>30</sup> Kohno et al. 2003, p.4.

<sup>31</sup> Diebold 2003, p.4.

<sup>32</sup> Kohno et al. 2003, p.4.

<sup>33</sup> Diebold 2003, p.5.

<sup>34</sup> State of Maryland 2004, p.5, emphasis in original.

security of the voting system should be evaluated from the view-point that some precautions or systems will fail, and what is important is how well the systems and procedures in place detect, repair and recover from failures.<sup>35</sup>

Although RABA Technologies was critical of the findings, in particular what they refer to as the ‘false hypotheses’ in the Hopkins Report, they do applaud their efforts and recognise valid issues were raised. Furthermore, RABA Technologies, in conducting their own assessment of the Diebold voting systems, revealed considerable security risks. The focus of the assessment was to evaluate the security and robustness of the smartcards, the voting terminals, the server system, and the methods used to upload the election results. Although a simulated attack revealed deficiencies in the system, RABA Technologies asserted that each of the vulnerabilities has a ‘mitigating recommendation’ which if implemented would facilitate an election ‘worthy of voter trust’.<sup>36</sup>

The discussion will now turn to individual countries that have used electronic voting, including DRE and the Internet, to establish whether the concerns and issues raised were real or perceived.

---

<sup>35</sup> *ibid*, p.7.

<sup>36</sup> *ibid*, pp.3–16.

## Chapter Two: The American experience: DRE

The US Presidential election year of 2000 will be remembered for the controversy surrounding the contested election and hanging chads'.<sup>37</sup> So widespread was the discontent the US federal government enacted legislation to improve the nation's voting systems and provided funding for the replacement of old voting technology. There is a concern in the US that whilst the States receive federal funds to update their voting systems and adopt new technologies, they are neglecting the importance of adequate poll worker training to administer the systems in a sufficient manner.

In the lead up to the 2004 US Presidential election, an international human rights organisation, Fair Election International (FEI), invited independent observers to evaluate the upcoming election.<sup>38</sup> The following commentary is derived from FEI observation reports and data compiled by the Verified Voting Foundation (VVF) and Election Protection Coalition (EPC). The VVF, in conjunction with the EPC and its associated members, have developed the Election Incident Reporting System (EIRS). EIRS is an integrated set of computer tools for recording and analysing information about voting problems before, during, and after elections.<sup>39</sup>

### **Fair Election International general observations:**

The FEI delegation raised concerns regarding the lack of uniform standards in recruiting and training poll workers, with each county evaluated<sup>40</sup> having their own poll worker training and recruitment procedures, ranging from a minimum one hour per year, to once every three years, regardless of changes or complexity in election laws.<sup>41</sup>

In relation to electronic voting, the delegation noted two firms provide virtually all of the DRE machines used in the US, and like other commentators noted that the software used in the systems were proprietary, controlled by the manufacturer and not open to public scrutiny. Technicians addressing errors or malfunctions were accountable to the manufacturer and not election authorities and during demonstrations of DRE errors were noted. Concerns remained in relation to security of data transmission from polling places to tabulation centres.<sup>42</sup>

To illustrate the breadth of problems observed during the 2004 election, the following observation can be made. Around 43,000 incidents were reported and logged on EIRS, and although there was a great deal of concern surrounding the use of DRE, only a small number, approximately 2,300 or 5 per cent, related to voting machine problems (refer to table 1).

---

<sup>37</sup> Chad is a descriptive term for paper particles created when holes are made in paper, such as those produced with a hole punch. The word came to prominence during the 2000 presidential election due to the amount of voters leaving incompletely-punched holes, or hanging chads, making it difficult for election officials to determine the electors voting intent.

<sup>38</sup> The 20 observers from 15 countries consisted of civic leaders, parliamentarians, diplomats, lawyers, electoral officials, academic specialists and veteran election officials. Their evaluation of the electoral process was conducted in September 2004, two months prior to the presidential election in November. The delegation also evaluated and reported on the November election.

<sup>39</sup> <https://voteprotect.org/index.php?display=EIRHome>

<sup>40</sup> Arizona, Florida, Georgia, Missouri and Ohio.

<sup>41</sup> Fair Election International 2004a, p.6.

<sup>42</sup> *ibid*, p.7.

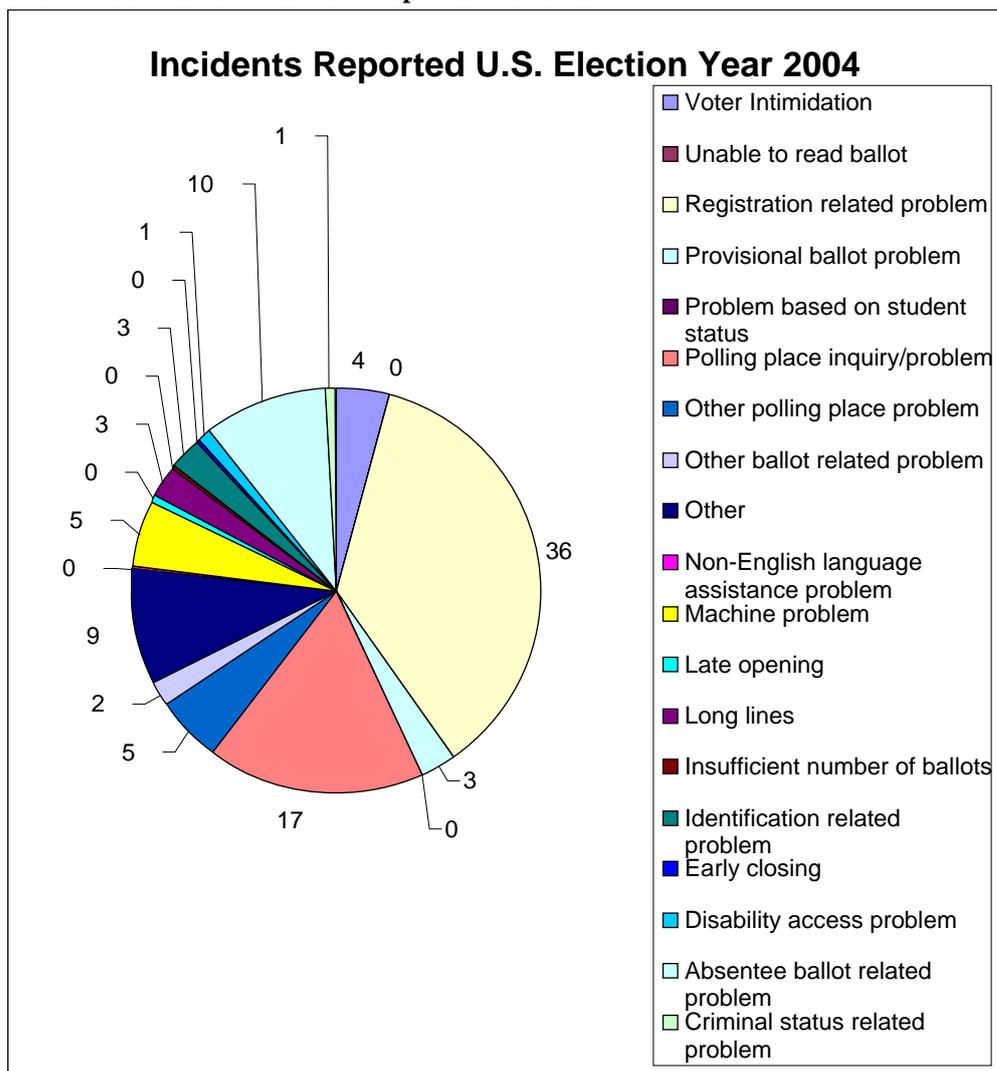
**Table 1: US Election Year 2004 Reported Incidents<sup>43</sup>**

<b>Incident Reported</b>	<b>Number</b>	<b>Percentage</b>
Voter Intimidation	1,764	4.12%
Unable to read ballot	51	0.12%
Registration related problem	15,404	35.96%
Provisional ballot problem	1,181	2.76%
Problem based on student status	74	0.17%
Polling place inquiry/problem	7,404	17.28%
Other polling place problem	2,248	5.25%
Other ballot related problem	794	1.85%
Other	3,896	9.09%
Non-English language assistance problem	111	0.26%
<b>Machine problem</b>	<b>2,293</b>	<b>5.35%</b>
Late opening	208	0.49%
Long lines	1,072	2.50%
Insufficient number of ballots	129	0.30%
Identification related problem	1,075	2.51%
Early closing	121	0.28%
Disability access problem	539	1.26%
Absentee ballot related problem	4,122	9.62%
Criminal status related problem	354	0.83%
<b>Totals</b>	<b>42,840</b>	<b>100.0%</b>

Although this is a crude measure, the data revealed an election system suffering more from a lack of administrative control and management, than a technological meltdown. The biggest area of concern, or number of incidents reported, related to elector registration problems, 36 per cent, followed by difficulties experienced at polling places, 17 per cent. Collectively, 95 per cent of reported incidents were associated with election management or procedural processes (refer to chart 1).

<sup>43</sup> Complete data set can be accessed at <https://voteprotect.org>.

Chart 1: US Election Year 2004 Reported Incidents<sup>44</sup>



A number of the incidents reported reflected a lack of knowledge on behalf of electors, and should/could have been directed to election officials for clarification and resolution. For example:

- Voter moved and wants to know in which precinct to vote.<sup>45</sup>
- Voter frustrated because he did not see registration deadline had passed.<sup>46</sup>

Conversely, there were reported incidents that reflected procedural flaws:

- Registered to vote before deadline but has not received voter registration card in the mail.<sup>47</sup>
- Registered to vote in Nov 2003. Has not received her registration card, when called to follow up, was told her registration was incomplete because she had not included her birth date on

<sup>44</sup> *ibid.*

<sup>45</sup> <https://voteprotect.org/index.php?display=EIRHome>. Case Number 12206.

<sup>46</sup> *ibid.*, 26704.

<sup>47</sup> *ibid.*, 13922.

the registration application. She believes she did include her birth date on the application. Also complained that it was very difficult to get through to the Supervisor of Elections office. She had not received any notice that her registration application was incomplete or deficient in any way.<sup>48</sup>

The 5 per cent of reported incidents associated with voting machines included concerns associated with the old 'punch card' systems, long lines to access voting terminals, poll-worker errors, non-working and insufficient numbers of DREs. For example:

- Poll workers are pressing the wrong precinct number. Poll-worker entered wrong precinct # for assisted voter. Voter's helper caught the error and when she brought it to the attention of the poll-worker, he said it did not matter. The voter's aid said it did as the voter's correct ballot would not be available.<sup>49</sup>
- Voter concerned because ballots not being scanned through machines; worried that vote will not be counted.<sup>50</sup>
- Optical scanner is rejecting ballots and poll workers have been collecting by hand. They were unable to fix it. It started at 7 a.m.<sup>51</sup>
- There were five machines at the polling place, none were working. Paper ballots were issued while workers made no attempt to have machines fixed.<sup>52</sup>
- She voted and before pressing the last button, checked back to see if the votes were recorded accurately and found that in some places "No Vote" appeared. She voted again and then pressed the final button.<sup>53</sup>

Although these incidents represented valid areas for concern, they did not reflect an electronic voting system that was in disarray or corrupt. There have been many well documented incidents of DRE failures, poor poll worker training, and a lack of understanding on the behalf of electors on how to use them, but to date, there have been no substantiated incidents of electoral fraud in the context discussed in chapter one.

The focus will now shift to three States, Ohio, Florida and Missouri, for a more in-depth analysis of the electoral process.

## Ohio

The FEI delegation evaluated Ohio, which is considered to be a highly contested marginal seat. The evaluation included ten polling places in Cuyahoga County, which includes Cleveland, and eight polling places in Franklin County. Voting systems varied from county to county, for example, in Cleveland the punchcard system was used, whilst Franklin used an older version of electronic voting machine. Independent observers, including the FEI delegation, were denied access to polling places and

---

<sup>48</sup> *ibid*, 14083.

<sup>49</sup> *ibid*, 58131.

<sup>50</sup> *ibid*, 42970.

<sup>51</sup> *ibid*, 54919.

<sup>52</sup> *ibid*, 55442.

<sup>53</sup> *ibid*, 59450.

counting centres throughout the State, with one exception, a local poll judge in Franklin County who invited the group inside a polling place. Predominately though, the delegation was restricted to talking to voters as they emerged from the polls, election authorities, civil society organisations, party officials and the media. The delegation noted the lack of transparency in the electoral process, especially when compared to other States visited by FEI delegations where independent observation was permitted.<sup>54</sup>

The FEI delegation observed a system failure in Ohio, where an optical scan machine incorrectly added 3,893 votes to one candidate in a polling place where only 800 voters registered. The error was discovered and remedied immediately using the residual vote methodology discussed in chapter one.<sup>55</sup>

Other irregularities observed in Ohio included ‘a polling station opening late, a polling station without a judge,<sup>56</sup> several reports of voting machines being broken and then replaced, and the failure of electronic voting machines’.<sup>57</sup> Long delays at nearly all polling places were also observed, in some cases in excess of two hours, with reports of up to six hours in other locations. In Cuyahoga County, the configuration and size of the ballots were confusing for voters and the ballot paper and punchcard machines did not line up correctly.<sup>58</sup>

The FEI delegation contended that efforts should be made to reduce the number of elections being conducted at the same time, reduce the size and complexity of ballots and called for the standardisation and simplification of ballot papers. In addition, the FEI delegation was given limited and restricted access to the ballot counting process and was not permitted to witness any downloading of electronic ballots from voting machines.<sup>59</sup>

According to the EIRS data, a total of 4,168 incidents were logged, of these 272 or 7 per cent were voting machine related. The greatest number of incidents reported, 1,165 or 27 per cent, were associated with elector registration problems (refer to chart 2).

---

<sup>54</sup> Fair Election International 2004b, p.11.

<sup>55</sup> *ibid*, p.5.

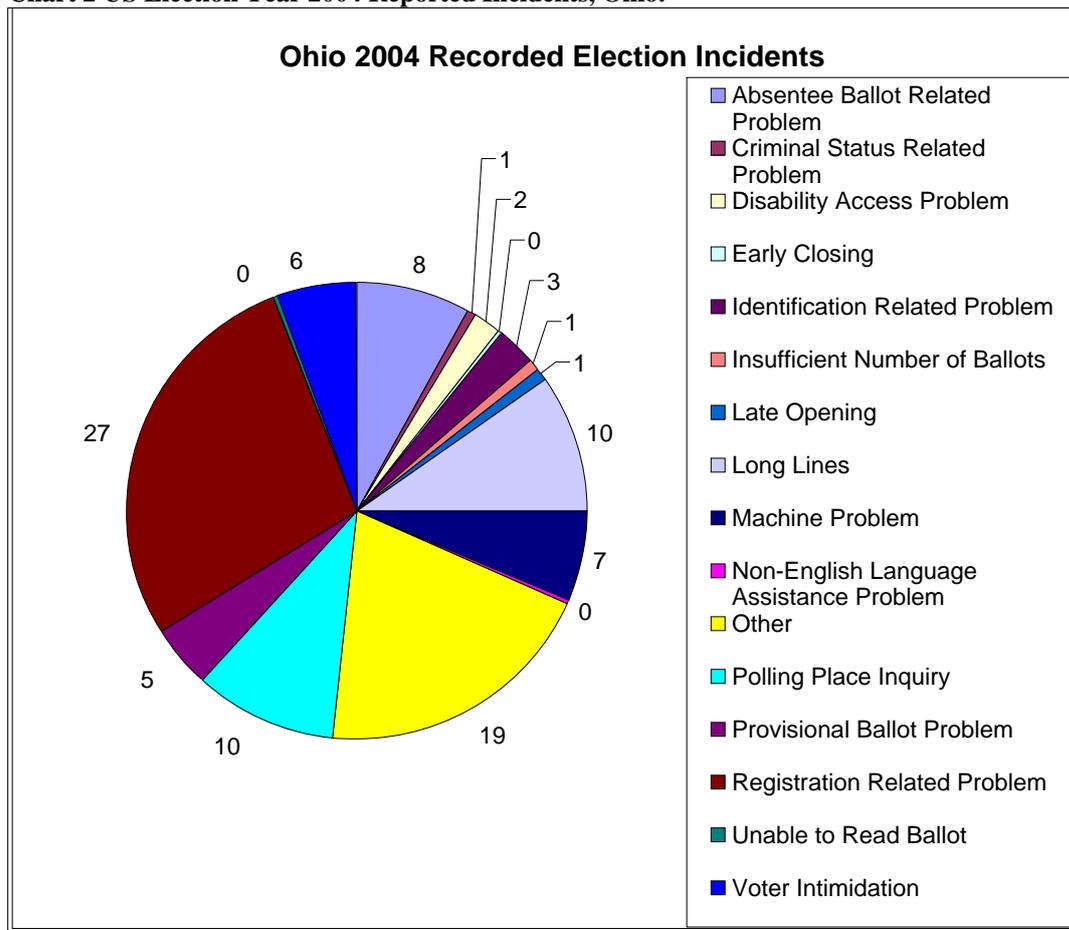
<sup>56</sup> Judges are responsible for the administration of election procedures in the polling place on election day. They are in the position of ensuring the election process is administered fairly and in accordance with election laws (Rockford Board of Election Commissioners, viewed 22 August 2006 <<http://www.voterockford.com/getInvolved/becomeJudge.aspx>>.

<sup>57</sup> Fair Election International 2004b, p.12.

<sup>58</sup> The delegation witnessed some ballots being 16 pages in length (Fair Election International 2004b, p.6).

<sup>59</sup> Fair Election International 2004b, p.13.

Chart 2 US Election Year 2004 Reported Incidents, Ohio.<sup>60</sup>



## Florida

The FEI delegation chose Florida due to its prominence in the 2000 constitutional crisis and high level, widely publicised voting system failure. The delegation observed the election process in three counties: Miami-Dade; Broward, Ft. Lauderdale; and Leon, Tallahassee. Initially the delegation was denied access to polling places in Miami and Broward counties and was allowed only limited and escorted access to some locations after last minute discussions with election officials. In contrast, Leon County provided full access and cooperation. As is the norm in the US, different voting equipment was used across the counties, namely a combination of DRE voting machines and optical scan machines.<sup>61</sup>

The delegation contended that had the margin of victory been as close as it was in 2000, ‘the irregular use of provisional ballots, lack of control over the distribution of absentee ballots, and problems with the registration process would have thrown the electoral process into doubt’.<sup>62</sup>

<sup>60</sup> Complete data set can be accessed at <https://voteprotect.org>.

<sup>61</sup> Fair Election International 2004b, p.8.

<sup>62</sup> *ibid*, p.9.

Specific incidents included a ‘software glitch’ experienced in Broward County that resulted in the miscalculation of thousands of absentee ballots. Fixing the software glitch resulted in restoring 32,000 ‘yes’ votes to one of the amendment questions being voted on that day. The problem was attributed to ‘human error’; a technician failed to adjust the software on the OSM to cater for the number of ballots received and it ceased counting at a certain threshold.<sup>63</sup>

In all three counties very long lines to enter the polling places were observed, on occasion electors queued for up to three and a half hours. Delays in voting were believed to be a result of an inadequate number of voting machines and lengthy ballots. For example, in Miami-Dade the ballot consisted of 27 questions over nine pages, resulting in voters taking approximately 45 minutes to cast their vote. In addition and again at Miami-Dade, the delegation noted that at some polling places officials failed to accurately record the number of electors who registered to vote and consequently could not reconcile the number of electors with the number of votes recorded on each DRE. In one Miami polling place, Olinda, where records of the number of registered voters were compiled, a discrepancy was noted between the number of votes recorded on the DRE and that of the register. Although poll workers could not explain the discrepancy it was only small at 23 votes.<sup>64</sup>

Also noted was confusion for both voters and poll workers regarding the administration of provisional ballots. In some instances poll workers were too quick to distribute a provisional ballot without adequate attempts to resolve issues. There was also uncertainty amongst poll workers regarding the rules for requiring and presenting identification. For example, in Broward and Miami-Dade, it was observed that many poll workers mistakenly believed that the law requires voters to produce some form of identification. In Broward, there were reports that up to 58,000 electors did not receive their absentee ballot, and when some of these voters attended a polling place they were advised that their ballot had been received by the elections department.<sup>65</sup>

According to the EIRS data, a total of 5,295 incidents were logged, of these 362 or 7 per cent were voting machine related. The greatest number of incidents reported, 1,416 or 27 per cent, were associated with elector registration related problems. These figures were identical in percentage terms as those observed in Ohio. In relation to absentee ballots there was a significant increase in reported incidents, 18 per cent, compared to Ohio, 8 per cent. The data tends to support the observations made by the FEI delegation that a considerable number of electors may not have received their absentee ballots (refer to chart 3).

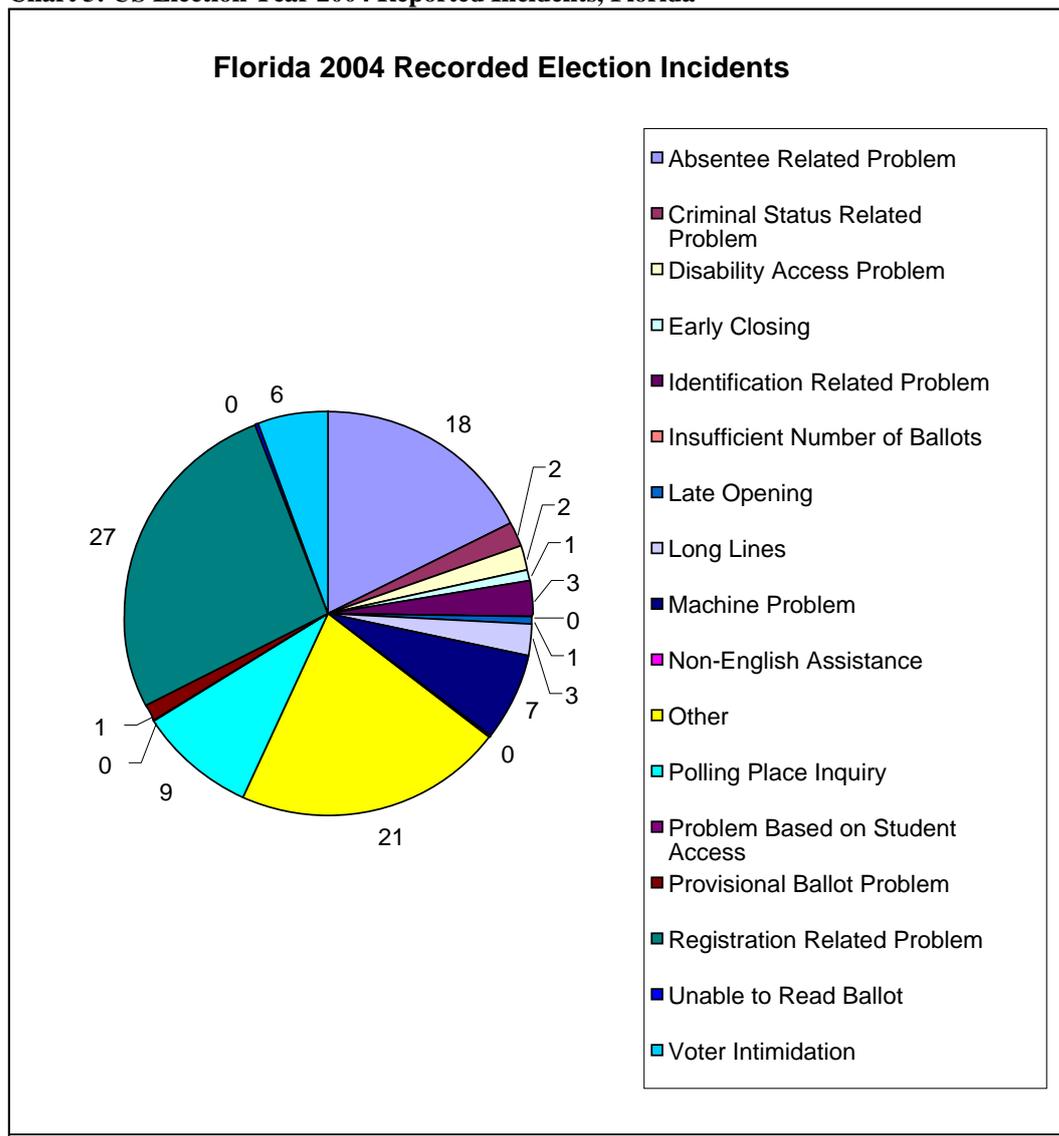
---

<sup>63</sup> *ibid*, pp.5-6.

<sup>64</sup> *ibid*, p.9.

<sup>65</sup> *ibid*, p.10.

Chart 3: US Election Year 2004 Reported Incidents, Florida<sup>66</sup>



## Missouri

Missouri was chosen by the FEI delegation because in the 2000 election thousands of eligible St. Louis electors were unable to vote due to being incorrectly placed on inactive voter lists. The delegation observed the election process in Boone County, St. Louis City, and St. Louis County. In Missouri, State election law explicitly permits international observation. In Boone County full access was granted to all 90 polling places and in St. Louis City full access was granted to all 200 polling places. However, the Board of Election Commissioners for St. Louis County, despite the legal requirements to the contrary, limited access to just two polling places and restricted the delegation’s activities and questions.<sup>67</sup>

In St. Louis City and St. Louis County, the delegation observed electors queued for up to three hours in duration throughout the day. The delegation observed ‘serious flaws’, including inadequate preparation of polling staff and judges, and identification requirements that go beyond those stipulated in HAVA. There were incidents where

<sup>66</sup> Complete data set can be accessed at <https://voteprotect.org>.

<sup>67</sup> Fair Election International 2004b, p.15.

people with no identification were allowed to vote but their votes were not included in the final count. There were also irregularities in the way ballots were handled in an insecure manner, including the emptying of ballots onto tables, allowing them to fall to the floor, and then placing them into another box for transportation to the Election Commission office. This process was being conducted in polling places that had poor visitor logs and uncontrolled movement of people.<sup>68</sup>

There were also incidents of Election Commission officials manually replicating ballots they had determined had been inadvertently cast on the incorrect ballot paper. The delegation considered there was poor coordination of resources with some voting precincts over staffed and under utilised, whilst others were struggling with demand.<sup>69</sup>

Although the delegation noted irregularities, they did not suggest they were systemic, rather a result of poor poll-worker training. They cited the example of late opening of a polling place and electors being misinformed about their votes being counted if they voted at a place other than their correct polling location. On one occasion an elector was misinformed about the correct polling place, only to find her polling place after the polls closed. Other incidents included 'group voting', whereby more than one eligible elector was present at a polling booth at a particular time.<sup>70</sup>

In contrast, Boone County was considered to be an exemplar in election coordination, as it was well organised and successfully run. Only minor, easily resolved incidents were observed, such as partisan campaign material being placed too close to polling locations and at some locations the slow processing of electors. There were also a few incidents of inconsistencies in the instructions given to voters by poll workers on how to complete a ballot.<sup>71</sup>

The delegation attributed the success of the election in Boone County to factors such as high retention rates of poll workers from election to election, in-depth and high quality poll worker training programs, and adequate resources for polling judges including laptop computers, mobile phones and pagers for communication, and instant access to the voters' database at the County Clerk's office. This enabled polling judges to quickly establish the eligibility of electors, thus reducing the need for and use of provisional ballots.<sup>72</sup>

According to the EIRS data, a total of 798 incidents were logged in Missouri, of these 8 or 1 per cent were voting machine related. These figures were the least in aggregate and voting machine specific terms. The greatest number of incidents reported, 325 or 41 per cent, were associated with elector registration related problems. This figure represented a marked increase, 14 per cent, compared to Ohio and Florida, with both States recording figures of 27 per cent. The data tends to support the observations made by the FEI delegation that in the 2000 election thousands of eligible St. Louis voters were unable to vote due to being incorrectly placed on inactive voter lists and such irregularities might be evident in the 2004 election. In relation to absentee ballots there was a significant decrease in reported incidents, 7 per cent, compared to Florida 18 per cent, and inline with Ohio, 8 per cent. (refer to chart four).

---

<sup>68</sup> *ibid*, p.16.

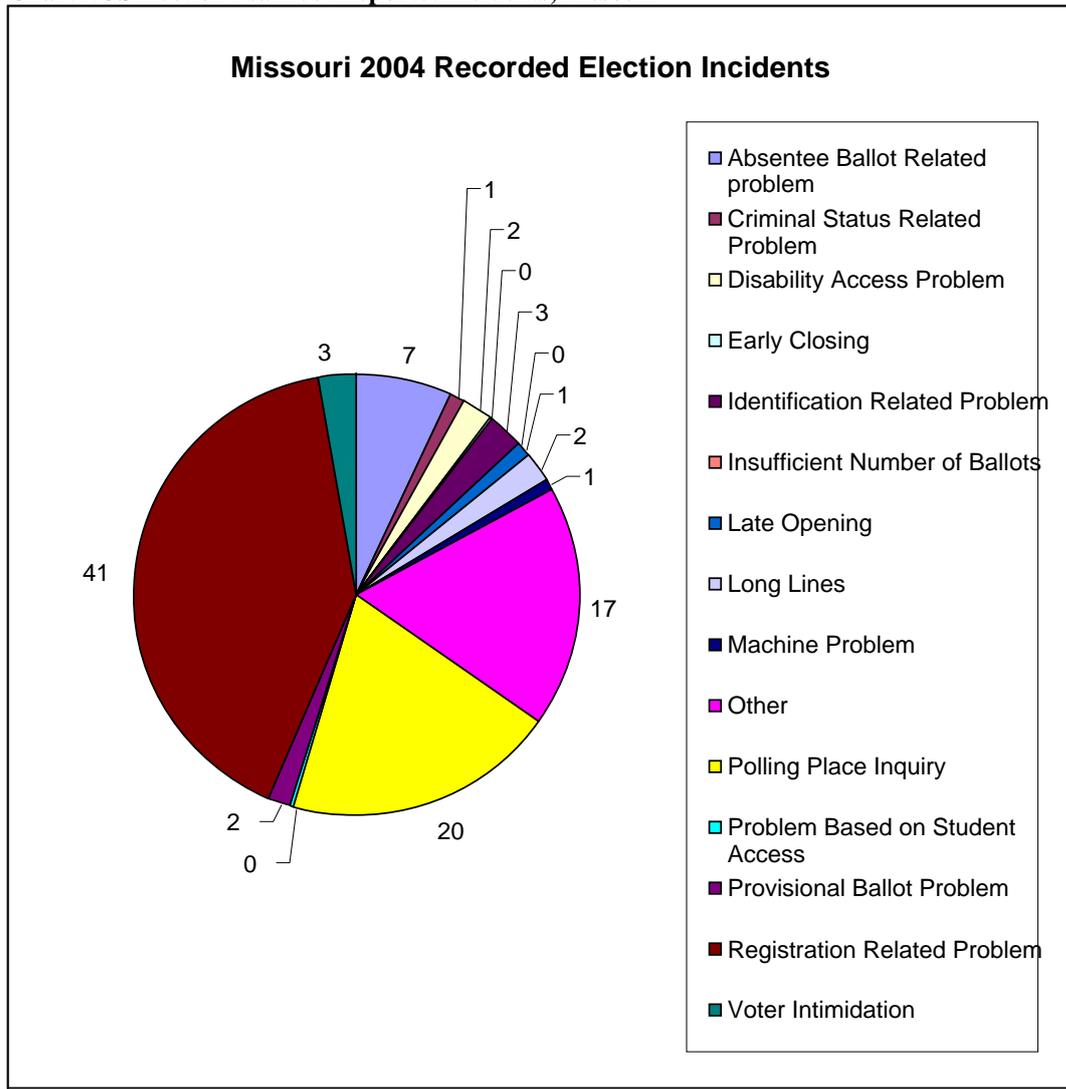
<sup>69</sup> *ibid*.

<sup>70</sup> *ibid*, pp.16–17.

<sup>71</sup> *ibid*, p.17.

<sup>72</sup> *ibid*.

Chart4:USElectionYear2004ReportedIncidents, Missouri<sup>73</sup>



The case studies reveal an interesting picture of the US election process and how the three States, Ohio, Florida, and Missouri, compare against the country as a whole. There appears to be a correlation in the data suggesting that all three States suffer from election management and procedural failure. Collectively, problems associated with absentee ballots, provisional ballots, and elector registration, accounted for over 40 per cent of reported incidents. Voter intimidation was nearly as big a dilemma as voting machine problems, whilst long lines, polling place inquiries, and ‘other’ problems accounted for over 30 per cent of other reported incidents (refer to table 2).

<sup>73</sup> Complete data set can be accessed at <https://voteprotect.org>.

**Table 2: Overview of reported incidents in the US 2004 election**

<b>Issue</b>	<b>U.S</b>	<b>Ohio</b>	<b>Florida</b>	<b>Missouri</b>
Absentee ballots	10%	8%	18%	7%
Provisional ballots	3%	5%	1%	2%
Elector registration	36%	27%	27%	41%
<b>Total</b>	<b>49%</b>	<b>40%</b>	<b>46%</b>	<b>50%</b>
Long lines	3%	10%	3%	2%
Polling place inquiry/problem	17%	10%	9%	20%
Other	9%	19%	21%	17%
<b>Total</b>	<b>29%</b>	<b>39%</b>	<b>33%</b>	<b>39%</b>
Voting machine problem	5%	7%	7%	1%
Voter intimidation	4%	6%	6%	3%
<b>Total</b>	<b>9%</b>	<b>13%</b>	<b>13%</b>	<b>4%</b>

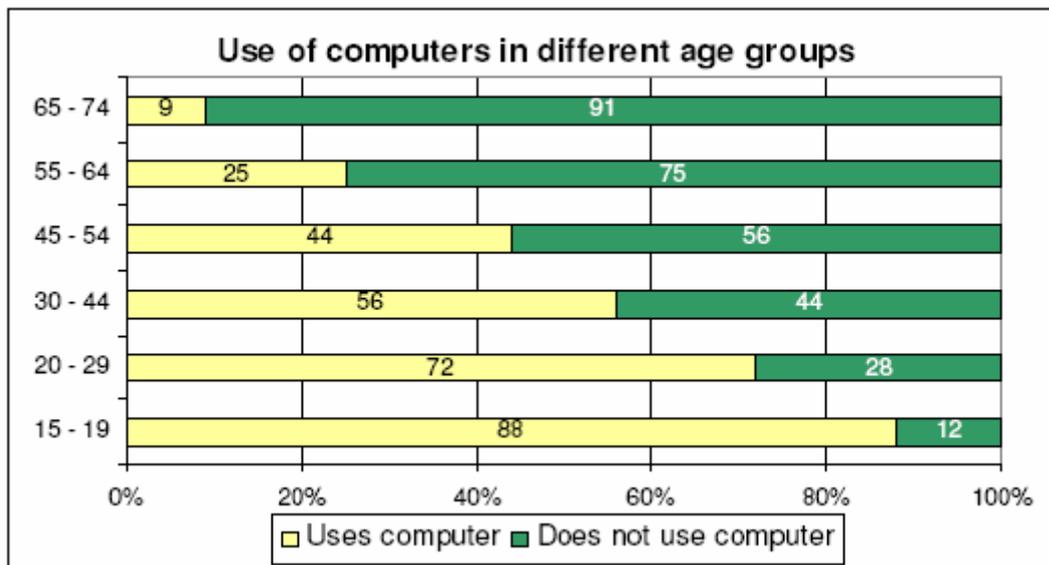
## Chapter Three: The Estonian Experience: Internet Voting

Estonia is a parliamentary democracy which conducted a country wide Internet voting trial in October 2005. Estonia was chosen for a case study due to the decision to offer Remote Internet Voting (RIV) to all eligible electors, which allows for a clearer picture of perceived security threats or impediments to successfully adopting the Internet to facilitate elections.

Estonia has a population of approximately 1.4 million, with a land area of approximately 45,226 km<sup>2</sup>. Although it is geographically small in comparison to Western Australia (WA), Estonia provides an insight into how an Internet voting system might work within a political jurisdiction of a comparable population base.

Estonia has an information technology saturation rate comparable to Australia, providing valuable comparison insights into possible future usage trends should Internet voting be offered in WA. Australian data for 2004–2005 suggests that 67 per cent of Australians had access to a computer at home, and 56 per cent had home Internet access.<sup>74</sup> Data compiled in 2005 suggested over 50 per cent of Estonian residents used the Internet, 40 per cent of households had a home computer, with 81 per cent of those connected to the Internet. In addition, all schools and public libraries had internet connections.<sup>75</sup> As is the case in other countries, computer usage was concentrated in younger age groups (refer to table 3).

**Table 3: Estonian computer usage by age group**<sup>76</sup>



<sup>74</sup> ABS 2005, cat 8146.0.

<sup>75</sup> Estonian National Electoral Committee 2005b, p.6.

<sup>76</sup> *ibid.*

## Contextual information

Estonia views itself as an innovative and successful 'e-state', whose relatively small population has genuinely easy and widespread access to the Internet. Increasing numbers of e-services have been established with their availability expanding year by year. The implementation of Internet voting is not intended to replace current voting systems in Estonia. As in other countries, Internet voting is a supplementary addition.<sup>77</sup>

In recent years Estonia has undergone fundamental reforms, in particular the introduction of identity (ID) cards. Since 2002, it has been mandatory for Estonian residents to hold an ID card and due to the relatively small population, take up has been rapid, with over 900,000 cards being issued. The ID card is fundamental to the Internet voting process as it provides a means to remotely authenticate electors, and provides a unique digital signature for secure verification.<sup>78</sup>

Due to Estonia's largely urban population, approximately 67 per cent, the use of the Internet linked to the country's mandatory ID card was considered advantageous. In addition, projects such as 'village road', which endeavours to spread Internet access and user education to regional areas, or approximately 33 per cent of the population, was a fundamental part of the Internet voting trial. The village road project was supported through the provision of more than 1,000 free Internet access points, in addition to access through public libraries.<sup>79</sup>

The introduction of ID cards has become an integral part of Estonian life, and is linked to a range of e-services, including the identification systems of private banks. The ID card has embedded electronic identities and digital signatures and is also used for, among other things, as a library card, public transport travel card, and health insurance membership card. The provision of e-services is proving popular, with 72 per cent of adult Internet users using online banking services, and 76 per cent of tax declarations submitted electronically in 2005.<sup>80</sup>

Upon issue each ID card has a 'digital certificate'<sup>81</sup> embedded for these purposes, and each recipient is given two PIN codes, one for digital identification and the other for digital signing. Under the Estonian *Digital Signature Act 2000*, a digital signature has the same legal status as a hand-written signature.<sup>82</sup>

---

<sup>77</sup> Estonian National Electoral Committee 2005b, p.4.

<sup>78</sup> *ibid*, p.4.

<sup>79</sup> *ibid*, p.5.

<sup>80</sup> *ibid*, p.8.

<sup>81</sup> An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify a user's identity, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. Definition supplied by Webopedia, viewed 01 August 2006 <[http://www.webopedia.com/TERM/d/digital\\_certificate.html](http://www.webopedia.com/TERM/d/digital_certificate.html)>.

<sup>82</sup> Estonian National Electoral Committee 2005b, pp.8–9.

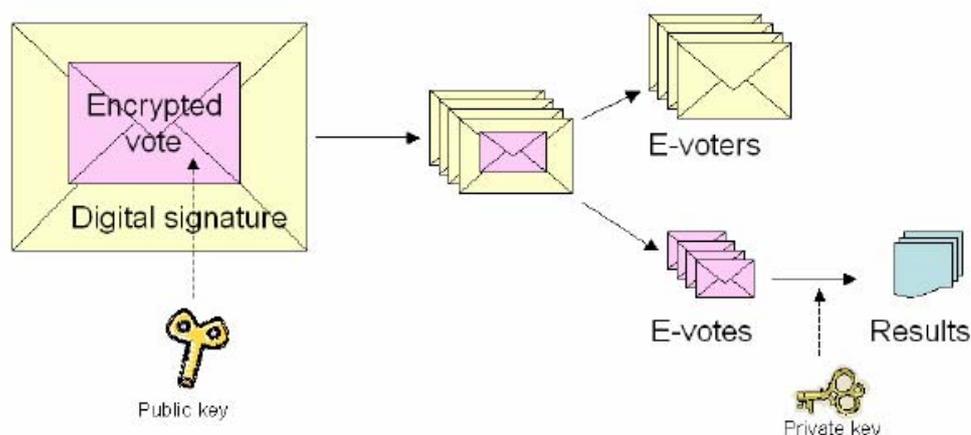
## E-voting project

The e-voting project started in 2003 in preparation for the 2005 trial, with three preconditions required to be satisfied before implementation: the existence of a legal basis; widespread use of ID cards; and the existence of electronic polling lists<sup>83</sup>

Estonia has been using a ‘double envelope’ voting system in local elections for many years, which allows electors to cast a ballot outside their ‘polling division of residence’, and provides for the elector to cast one ballot anonymously.<sup>84</sup> The double envelope method requires an elector to place their marked but unidentifiable ballot paper into a small inner envelope. This envelope is then placed into a larger outer envelope on which the elector identifies themselves and signs a declaration on the outer envelope stating they are entitled to vote. Upon receipt of the envelope the authority checks the declaration against the electoral roll. Once an elector’s right to vote has been established the inner envelope is removed and placed unopened into the ballot box for later counting.

Estonia has drawn on this methodology in designing the e-voting system (refer to diagram 1).

**Diagram 1: General description of e-voting and the envelope method.**<sup>85</sup>



The Estonian e-voting system replicates the double envelope model described above. The encrypted vote can be thought of as the ‘inner envelope’ and the digital signature can be thought of as the ‘outer envelope’. The model was developed due to its perceived simplicity in system architecture and comprehensibility, and parallels can be drawn with the ‘traditional’ voting system used in Estonia. Moreover, the system incorporates the full use of digital signatures, ‘public key’ cryptography and encryption<sup>86</sup> for security and authentication purposes.<sup>87</sup>

<sup>83</sup> Estonian National Electoral Committee 2005b, p.20.

<sup>84</sup> *ibid*, pp.22–23.

<sup>85</sup> *ibid*, p.23.

<sup>86</sup> Public Key Encryption—A cryptographic system that uses two keys, a public key known to everyone and a private or secret key known only to the recipient of the message. Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use. The only noted difficulty with public-key systems is that a user needs to know a recipient's public key to encrypt a message for that person. To address this issue new LDAP technology promises a global registry of public keys. Definition supplied by Webopedia, viewed 02 August 2006 <[http://www.webopedia.com/TERM/p/public\\_key\\_cryptography.html](http://www.webopedia.com/TERM/p/public_key_cryptography.html)>.

In the Estonian case, electors logged onto the election website on advance polling days and identified themselves using the certificate embedded on their ID card. Upon clarification of their identity a candidate list was displayed for their consideration. The elector made their choice from the list and confirmed their selection by signing their vote digitally using the embedded certificate on their ID card. Notification of their successful vote was then displayed on the website page.

The digital signatures (the outer envelope identifying the voter and their eligibility) were separated from the encrypted votes (the inner envelope), and elector lists were updated from the digital signatures received in much the same manner as that associated with the ‘traditional’ double envelope method. The encrypted votes, which were then separated from the identity of the elector, were forwarded to the vote counting application for tabulation. To keep the identity of the elector anonymous, the system was designed so that at no point in the voting process did any party have the digitally signed e-vote and the private key to unlock it.<sup>88</sup>

The Estonian model tackled the issue of coercion and vote buying by allowing individuals to change their e-vote by completing the whole process again during the advance polling period. Allowing multiple voting, usually considered a crime, negates concern over vote buying and coercion as it is impossible to convince any would-be voter purchaser that no alternative vote would be cast, as subsequent votes cancel previous votes. In relation to coercion, it is thought that once the undue influence has gone, an alternative and correct preference vote can be cast.<sup>89</sup>

The system also gave priority to ‘traditional voting’, so in the event an elector attended a polling place during the advance polling period any electronic vote previously cast was deleted. This also allowed, in the event of the e-voting system being seriously compromised, for all electronic votes to be declared invalid and for those electors to cast a ballot the traditional way.<sup>90</sup> Presumably this would require verification of identity at the polling place so as to ensure the security of the voter’s intention.

These proposals were opposed by Estonian President Arnold Rüütel on the grounds that it violated the constitutional principles of uniformity and equality amongst voters, as voters using traditional paper ballots were not afforded these options. The issue was decided in the Supreme Court in favour of allowing multiple votes and primacy of traditional voting.<sup>91</sup>

Additionally, the Estonian National Electoral Committee (NEC) took the following steps to protect the integrity of the election system. The requirement that e-voting take place between the 6<sup>th</sup> and 4<sup>th</sup> day prior to Election Day was incorporated into the electoral legislation. This stipulation was done to provide sufficient time for the electoral authority to produce a current electoral roll showing all those who have already cast an e-vote, thus preventing multiple voting.<sup>92</sup>

---

<sup>87</sup> Estonian National Electoral Committee 2005c, p8.

<sup>88</sup> Estonian National Electoral Committee 2005c, pp.8–9.

<sup>89</sup> *ibid*, p.6.

<sup>90</sup> *ibid*, p7.

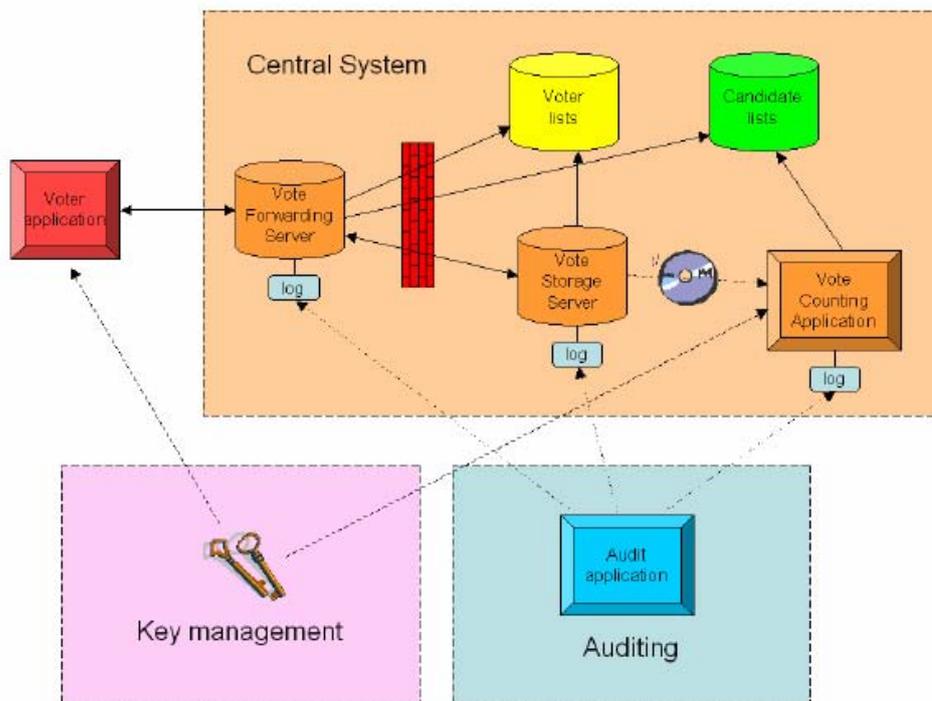
<sup>91</sup> European Commission 2005; & Estonian National Electoral Committee 2005b, pp.19–20.

<sup>92</sup> Estonian National Electoral Committee 2005c, p7.

The Estonian system was transparent enough to enable a wide-range of specialists to conduct audits. In line with other commentators on Internet security, the NEC emphasize the fact that there are two parties involved in the process, the voter using their personal computer (PC) and the election authority using their server network. Of the two it is the elector's PC which is the most vulnerable to malicious attack.<sup>93</sup>

The Estonian e-voting system, or architecture, was comprised of different parties or users. The central components, illustrated in orange (refer diagram 2), were; the vote forwarding server (VFS); vote storage server (VSS); and the vote counting application (VCA). Of these components only the VFS was directly accessible through the Internet. The remainder were protected by a firewall. Other components consisted of the elector and their access application, in this case their PC. The key-management system produced a pair of keys for each vote cast, one public that was integrated into the electors PC and a second one private, delivered to the VCA. There was also an auditing system that logged transactions and information generated during the polling period to solve any disputes or complaints that might arise.<sup>94</sup>

**Diagram 2: Estonian e-voting and system architecture**<sup>95</sup>



The VFS provided an authenticity check on the eligibility of electors against the voter list, displayed the candidate lists, and accepted encrypted and digitally signed votes. The elector interacted with the system through the VFS to view the candidate list in their 'division of residence', and after due consideration made their choice, created and sent an encrypted and digitally signed vote. Upon receipt, the VFS immediately sent the vote to the VSS along with confirmation back to the elector that their encrypted vote had been received.<sup>96</sup>

<sup>93</sup> Estonian National Electoral Committee 2005c, p.7.  
<sup>94</sup> *ibid*, p10.  
<sup>95</sup> Estonian National Electoral Committee 2005b, p.24.  
<sup>96</sup> *ibid*.

The VSS received and stored all the encrypted votes, and at the end of the advanced polling period all repeated or non-conforming votes were deleted from the VSS and an audit log created of their existence for any future disputes. All eligible encrypted votes (inner envelopes) were then separated from the digital signatures (outer envelopes) that contain the elector's personal data and were then written to a compact disc (CD) for tabulation in the VCA. Once the CD was loaded into the VCA for tabulation, the system obtained the private key(s) to access and count the encrypted votes.<sup>97</sup>

Now that a picture has been developed of the architecture of the Estonian e-voting system, it is possible to look at the actual election statistics to gauge user levels and the opinions of e-voting commentators.

### The election results and management process

It is worth noting the Estonian government's efforts to inform and educate the public on how the system worked. This was accomplished through two trials of the system. The first was a pilot project in January 2005, where residents in the capital Tallinn participated in a simple referendum to decide the location of the 'Freedom Monument'. The system was implemented as a whole, including multiple voting, priority of paper ballots, and the public opening and demonstration of the cryptography key system. Numbers involved in this trial were quite small, perhaps due to the subject matter of the referendum and the fact that voting was not compulsory. Of the 396,010 residents in Tallinn, 1.5 per cent participated; of this figure 703 or 13.7 per cent used the e-voting system.<sup>98</sup>

The second trial involved public testing of the system between 26 September and 2 October 2005. The aim of this trial was to encourage people to identify and resolve any problems that emerged, for example the acquisition of necessary software, updating expired ID card certificates, and renewal of PIN codes prior to the actual election. The conditions during this period were designed to replicate an actual e-voting environment: electors had to identify themselves using their ID cards; a fictitious candidate list was generated; and the voter's choice had to be confirmed with a digital signature.<sup>99</sup>

In 2005, there were approximately one million eligible electors in Estonia out of a total population of approximately 1.3 million. The overall participation rate in the 2005 municipal elections was 502,504 votes, or 47 per cent. The e-vote participation rate was 9,681 votes cast. Of this figure 364 were multiple votes, and as such the last vote replaced the previous vote bringing the actual number of e-voters down to 9,317. Of this figure 30 were cancelled and not included in the final tally of 9,287, or 1.8 per cent of valid e-votes (refer table 4).

---

<sup>97</sup> Estonian National Electoral Committee 2005b, p24.

<sup>98</sup> *ibid*, p25.

<sup>99</sup> *ibid*.

**Table 4: e-voting Statistics Estonian Municipal elections 2005<sup>100</sup>**

Registered voters	1,059,292
Total votes cast:	502,504
Valid (e-votes includes)	496,336
Invalid	6,168
Turnout	47%
Number of e-votes cast	9,681
Repeated e-votes (more than one e-vote per voter)	364
Number of e-voters	9,317
e-votes counted	9,287
Cancelled e-votes	30
E-vote turnout	1.8%
Advance votes (e-votes included)	24%
E-votes among advanced votes	8%

## Critique

The NEC was praised for publishing their ‘E-Voting System Overview’ document, thus enabling interested parties to analyse and comment on the systems architecture. Jason Kitcat, an online consultant and researcher at the University of Sussex and ardent critic of electronic voting systems, acknowledged Estonia’s Linux-based system was the most secure to date, yet contended the option to cast multiple votes and/or paper ballots increased complexity levels and costs.<sup>101</sup>

In his online discussion forum, Kitcat contends the Estonian use of ‘public key infrastructure’ (PKI) based identity cards was a positive step to resolving authentication issues experienced in other countries. He did, however, raise concerns regarding the potential to commit an act of fraud once digital signatures are separated from votes. In essence, once the digital signature is removed from the encrypted vote its uniqueness and authenticity can no longer be verified, opening the potential for unsigned votes to be added, swapped, or removed from the system. Kitcat suggested the use of a unique number, such as a ‘timestamp’ in conjunction with a transaction audit log, should be added to each vote as a counter measure. Kitcat conceded that he was unaware if the Estonian model did or did not take this precaution. Nevertheless, he contended that the log system ‘is one of the best [he has] ever seen in an e-voting system’.<sup>102</sup>

Professor David Wagner of the University of California, Berkeley, outlined the same arguments against electronic voting as discussed in chapter one. However, in the absence of such events in the Estonian election, opined that when only a few citizens cast their vote online there is little incentive for hackers to exploit the vulnerabilities of the system.<sup>103</sup> While this might be true, it is an assumption only. In a nation of approximately 1.4 million people, and with the Internet being the only e-voting

<sup>100</sup> Estonian National Electoral Committee (2005a), full statistics can be found at <http://www.vvk.ee/english/results.pdf>.

<sup>101</sup> Jason Kitcat, Quoted in European Commission 2005.

<sup>102</sup> Kitcat 2005.

<sup>103</sup> Quoted in European Commission 2005.

method available, it would not be unreasonable to assume that people with malicious intent, sufficient hubris, motivation, and technological skill, may view the opportunity to disrupt the election with envious eyes. After all, there can only be one 'first' regardless of how big the second disruption might be.

An advantage of the Estonian system, one that enhances security and limits the potential for fraud, is that no password or 'voter identification number' (VIN) is required to be posted out to the elector. The sending of confidential information is not required due to Estonian citizens already having micro-chipped identity (ID) cards, and because they already know their PIN to access and use them.<sup>104</sup>

Although the security measures afforded by the use of electronic ID cards in Estonia can be considered a positive, such a method could prove problematic for other democracies, in particular in a country such as Australia where there has been a tradition of opposition to such propositions. Importantly, the Australian federal government is currently (2007) considering the introduction of an 'Access Card' as a means to streamline the delivery of government services, namely health and social security benefits. These services are presently provided through various government agencies often with their own entitlement card.

The mooted Access Card is intended to reduce the number of entitlement cards held by members of the public and to enhance data exchange between the various service providers and service users. The card is intended to be made 'available to people over 18 years of age...who are entitled to claim health or social service benefits from the Australian Government [and will have an individual's] name, address, details of children or other dependants, digitised photo, signature, card number, expiry date, gender, concession status and [a] Personal Identification Number (PIN)' embedded into its microchip.<sup>105</sup> Should such an initiative become a reality and Australian citizens embrace it, then the 'Access Card' could prove a useful vehicle, technology permitting, to conduct electronic voting over the Internet in the future.

---

<sup>104</sup> Sheeter 2005.

<sup>105</sup> Australian Government Office of Access Card [http://www.accesscard.gov.au/about\\_card.html](http://www.accesscard.gov.au/about_card.html).

## Chapter Four: The Indian Experience: EVM

India is an interesting case study, not just because it is the world's largest democracy, but because in 2004 it held its first all-electronic General Election. The sheer logistics of the election is worthy of merit alone (refer table 5). The General Election to the fourteenth 'Lok Sabha' (the House of People of the Indian Parliament) was conducted by the Election Commission of India (ECI) during April–May 2004. The General Election was scheduled to take place in October of that year, but was conducted earlier than planned due to an early dissolution of Parliament. Consequently, the ECI decided to hold elections for the 'Lok Sabha', State Legislative Assemblies of Andhra Pradesh, Karnataka, Orissa and Sikkim, and 15 by-elections in various states concurrently.

**Table 5: General Election 2004 India<sup>106</sup>**

<b>Lok Sabha General Election 2004</b>	
Total Seats	543
Total Number of candidates	5,398
Registered electors	671,524,934
Number of Polling Places	700,000
Number of election personnel engaged	Approx. 4 million (excluding police)
Number of Electronic Voting Machines	1.075 million
Direct expenditure	Approx. Rs 13000 million (AUD 404 million, or .60 cents a vote)
Total votes polled	387,453,223
Elector turnout	56%
Amount of paper saved	8,000 metric tonnes

Like other democracies, India is striving to modernise and streamline its voting system through the adoption of electronic technology. India used a form of DRE that had been developed and manufactured by two government controlled companies, Bharat Electronic Limited (BEL) and the Electronics Corporation of India Limited (ECIL). During the 2004 election more than one million units were manufactured and distributed across India.

India had been using Electronic Voting Machines (EVM) since 1998, after an amendment to *The Representation of People Act 1951*. The first trial was small in scale; EVMs were only used in 16 Assembly constituencies during the 1998 State Legislative Assembly Elections. In contrast, EVMs were used throughout the country during the 2004 General Elections.<sup>107</sup>

<sup>106</sup> Election India (2004) *Election News Feb–June 2004 & Election 04 Facts and Figures* viewed 25 August 2006 <[www.eci.gov.in](http://www.eci.gov.in)>.

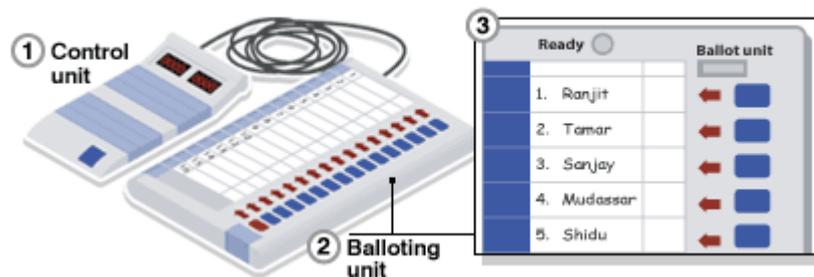
<sup>107</sup> Election India 2004.

## The Indian Electronic Voting Machine (EVM)

The approach adopted in India was to develop a system that was simple to use, understand, and not reliant on sophisticated architecture or software. One online 'blog' site, 'Techaos', received a posting comparing the Indian EVM with the Diebold system commonly used in the US, which argued the Diebold system was too complex for a straight forward task such as voting. This was because the Diebold system incorporates Windows CE, modems, PCMCIA storage cards, touch screen graphical user interface (GUI), on-screen writing facilities, voice guidance systems, multiple languages, encryption, centralised voting servers, voting wizards, SQL servers and backup servers, all of which were considered to increase costs and security vulnerabilities.<sup>108</sup>

Conversely, the Indian EVM consisted of two devices connected by a 5 meter cable (refer to diagram 3). One part was controlled by the election official, the other by the elector. The EVM ran on a battery, perhaps essential in a country with a large proportion of people living in remote and rural constituencies where electricity infrastructure is poor. The voting unit had a button next to the name of each candidate; in addition, each candidate had her/his party symbol next to their name so that even if the elector could not read, he/she could still vote for their preferred candidate. The symbols, easily recognised by electors, were approved by the ECI and were unique to a particular party.

**Diagram 3: India's Electronic Voting Machine**<sup>109</sup>



1. Control unit. Polling station staff press a button to release a ballot for each voter entering the booth. There is also a "close" button, which, once pressed, prevents any more votes being cast.
2. Balloting unit - this is the equivalent of a ballot paper.
3. The voter presses the button next to a candidate's name and the control unit records the vote. At the count, it says how many votes were cast and for whom.

The election process in India was similar to that observed in other countries. Electors identified themselves upon entry to a polling place, their finger was marked with a special and difficult to remove ink (a precaution against multiple voting), electoral officials pressed a button on the control unit to release a ballot (activate the system), the elector voted in a booth by pressing the button next to their preferred candidate, the balloting unit lit up next to the chosen candidate and sounded a long continuous beep to indicate a selection had been made.

<sup>108</sup> <http://techaos.blogspot.com/2004/05/indian-evm-compared-with-diebold.html>

<sup>109</sup> [http://news.bbc.co.uk/1/hi/world/south\\_asia/3493474.stm](http://news.bbc.co.uk/1/hi/world/south_asia/3493474.stm)

At the end of the voting period election officials, observed by political party officials, made a note of the total number of votes cast on each EVM. The EVM was then placed into a secure carry case and transported to the nearest District Headquarters for later counting. The counting of the votes commenced at the prescribed time, after election officials clarified that the recorded number of votes on each EVM at the point of departure, remained the same upon arrival at the counting destination. To count the votes a seal was broken on the EVM control unit and the results button was depressed to release the information.

## How the system fared

Eric Weiner (2004) writing in the online magazine *Slate*, compared the Indian EVM experience with the ('mostly urban legend') zero gravity pen being developed by NASA for use in space. NASA spent millions on the project that the Russians solved for the fraction of the cost by using a lead pencil. It appears history is repeating itself, with the American DRE costing approximately \$3,000 US per unit, compared to approximately \$200 US for India's EVM.

India can be considered a quiet achiever in the realm of electronic election modernisation. Its experiment resulted in approximately 380 million electors casting a vote on one of the 1 million plus voting machines in the world's largest experiment in electronic voting to date. Although the process was not perfect, it was considered a success.<sup>110</sup>

While the US agonized over touch screens and paper trails, India developed a system that overcame security, one of the biggest barriers facing electronic voting. As previously noted, the EVM was not reliant on multiple applications or software; it was configured to accomplish the simple task of counting votes, and as such, avenues to corrupt the system were reduced.<sup>111</sup>

For example, the Hopkins Report argued that DRE systems could be manipulated by 'malicious insiders' who tamper with the software to affect the results of the election to favour a particular candidate.<sup>112</sup> In relation to the Indian EVM this was not an issue, because candidate lists were not pre-installed; rather, candidate names were written on slips of paper that could be inserted in any order on the day of the election. Thus unscrupulous politicians with assistance of an 'insider' could not rig the machine at the factory as they did not know which button would be assigned to which candidate.<sup>113</sup> In addition, a 'malicious insider' would also need to ensure that the corrupted EVM was sent to the correct polling place to affect the fraud, which in India, was one of 700,000. Another safeguard built into the Indian EVM, either by design or default, was that the software was embedded onto a microprocessor that could not be reprogrammed.<sup>114</sup>

These measures taken together are sufficient to reduce the occurrence of what some computer scientists call 'wholesale fraud', or tampering with the software at point of manufacture. It has been suggested that the Indian EVM, due to its basic design, was less vulnerable to wholesale fraud, whereas the American DRE with its complicated

---

<sup>110</sup> Weiner 2004.

<sup>111</sup> *ibid.*

<sup>112</sup> Kohno et al. 2003, p.3.

<sup>113</sup> Weiner 2004.

<sup>114</sup> Kripalani 2004.

design and numerous lines of code was more susceptible.<sup>115</sup> NN Simha, General Manager of Bharat Electronic Limited, based in Bangalore, was confident that the EVM was tamper proof; Abhijit Dasgupta, Karnataka's Chief Electoral Officer, contended the machines would do away with mistakes; and Judge K Shridhar Rao, in an election dispute, ruled rigging of EVMs was not possible.<sup>116</sup>

There were concerns relating to 'retail fraud', or the tampering with the machines on an individual basis. However, given that there were over 1 million machines in use, spread over 700,000 locations, it would require a significant amount of time and resources to affect a change in the democratic process.

Although officials in India were pleased with the EVM and confident the system was safe from tampering, not everyone agreed. During the election period (20 April–10 May 2004) there were reports of faulty starts, voter confusion, and at least one known case of vote tampering.<sup>117</sup> According to Frederik Noronha, a myth developed around EVMs that they were tamper proof, but this assertion could not be independently verified as the source code had not been made public.<sup>118</sup> This line of argument, that propriety software precludes independent verification, resonates from Washington to Delhi.

India has a reputation for violent elections and 2004 was no different, with reports of individuals entering polling places and commandeering the EVMs and casting multiple votes. This led to re-polling being conducted in 1,879 voting booths.<sup>119</sup> This figure should be put into context; there were 700,000 polling places and the re-polling conducted represents less than one per cent (0.27 per cent). In another incident, in Bihar, an area that has been ravaged by electoral violence in the past, workers from a local political party seized control of the EVM and cast multiple votes. These incidents are an extension of India's well documented problem of 'booth capturing' and 'ballot stuffing' carried out by hired political thugs for political advantage.<sup>120</sup> These examples, though disturbing, were small, especially when one considers the size of the election and India's past experiences. Indeed, *The Times of India* noted that poll and sectarian violence was low compared to previous elections.

The design of the EVM and India's electoral system was intended to reduce fraudulent acts. Firstly, India's electoral system only permits a limited number of votes per polling place, previously 1,200, but in 2004 this was increased to 1,500, as a measure to limit the affects of 'ballot stuffing'. In the event of 'booth capturing' only a limited amount of fraudulent ballots could be cast. The EVM also had a built-in deterrent against 'ballot stuffing'; it only allowed a maximum of five ballots per minute to be cast, so in the event of a 'booth capture' the EVM could only record a limited number of votes.

---

<sup>115</sup> Weiner 2004.

<sup>116</sup> Beary 2004.

<sup>117</sup> Srinivasan 2004.

<sup>118</sup> Quoted in Srinivasan 2004.

<sup>119</sup> Srinivasan 2004.

<sup>120</sup> Rohde 2004.

Frederik Noronha asserted that the EVM had been designed by State controlled enterprises' and a small group of government people could, theoretically, change the code to manipulate elections.<sup>121</sup> This assertion may be dismissed given the result did not go the way of the ruling Bharatiya Janata Party (BJP). Of course, one could argue that the manufacturers, for whatever reason, conspired to overthrow the government of the day, although this would take us into the realm of deep conspiracy theory. Furthermore, such a scenario would surely draw wails of protest from the losing contender, and as this was not the case, one can assume the election result was widely considered free and fair.

A more credible theory is that the system worked well, and the result, thanks to the EVM, known sooner than had been the case in previous elections, was a true reflection of the 'will of the people'.

According to India's national press the result was an unexpected debacle for the government, with headline writers relaying the shock result in graphic terms. A constant theme in the reporting was the ruling BJP party was arrogant and disconnected from voters, in particular India's rural poor, and that the result was an unexpected shock. *The Telegraph's* Mahesh Rangarajan wrote '[t]here is little doubt the verdict was stunning and momentous. Its scale left even seasoned observers stunned, while all pollsters ran for cover'.<sup>122</sup>

Although the media was unprepared for the result, there was no suggestion that anything untoward took place in relation to the EVM. In other words, there was no suspicion of 'wholesale fraud'. Conversely, 'retail fraud' was an issue, although not to the extent that it affected the outcome of the democratic process, nor were its incidents a direct result of the introduction of EVM. On the contrary, 'booth capturing' and 'ballot stuffing' is a practice that evolved prior to the introduction of electronic voting technology, and if anything, the 2004 election was less violent than previous ones and the necessary re-balloting arguably more orderly.

---

<sup>121</sup> Quoted in Srinivasan 2004.

<sup>122</sup> BBC News Online. (2004). *Indian press consider surprise result*  
<[http://news.bbc.co.uk/1/hi/world/south\\_asia/3713599.stm](http://news.bbc.co.uk/1/hi/world/south_asia/3713599.stm)>.

## Chapter Five: The United Kingdom Experience: Multiple Voting Channels

### Background

The United Kingdom (UK) can be considered a pioneer in electoral reform due to its innovative approach in offering electors multi-channel voting options, extended voting hours and weekend ballots. The rationale for these innovative changes are many, but at the forefront is a desire to reverse the trend of declining elector participation, and to modernise a system that has been largely unchanged for over 100 years.<sup>123</sup> The UK conducted voting pilot schemes in 2000, 2002, 2003, 2004, and 2006. No pilots were conducted in 2001 and 2005 as these were General Election years. This paper will focus on the 2000, 2002, and 2003 pilot schemes, as these offered electors the chance to cast an electronic vote, whilst the 2004 and 2006 pilot schemes trialled entirely postal voting elections.

An important aspect of the UK electoral reform process was the establishment of an independent Electoral Commission in November 2000. The function and powers of the Commission are proscribed in the *Political Parties, Elections and Referendums Act 2000* (PPERA). The Act covers three broad themes and provides direction for the Commission's deliberations and work; modernisation of electoral law and practice, education, and regulation.

Another important aspect was the lobbying for electoral change by the Local Government Association (LGA), the Association of Electoral Administrators (AEA), and the Society of Local Authority Chief Executives (SOLACE). Their combined lobbying led to the development of the *Representation of the People Act 2000*.<sup>124</sup>

These two Acts provide the legislative framework for electoral reform in the UK. The *Representation of the People Act 2000* permits local government authorities to apply for permission to trial election pilot schemes, and the *Political Parties, Elections and Referendums Act 2000*, gives the Electoral Commission the authority to monitor and report on the schemes. The first successful applicants participated in trials in May 2000.

### The 2000 pilot schemes

In 2000, under the terms of the *Representation of the People Act 2000*, 44 local government authorities (authorities) sought permission to pilot new electoral arrangements at the 4 May 2000 elections. Of this number, 32 were successful, and between them they trialled 38 innovations. These included; 'postal votes on demand'; 'early voting'; 'all postal ballots'; 'electronic voting or counting'; 'extended polling hours'; 'mobile polling stations'; 'freepost communication'; and changing the polling day<sup>125</sup>.

Authorities participating in the pilot schemes were required to produce evaluation reports to determine whether the pilots were successful. In 2000, it was the responsibility of the 'Home Office' to produce the criteria for the authorities to base

---

<sup>123</sup> Local Government Association 2000.

<sup>124</sup> *ibid.*

<sup>125</sup> *ibid.*

their evaluations against. This responsibility is now part of the Electoral Commission's remit; the Commission was not in existence until the 30 November 2000.

The four questions contained in the Home Office circular RPA433 were:

- i. Was turnout higher than it would otherwise have been?
- ii. Did voters find the new arrangements easy to use?
- iii. Did the new procedures lead to any increase in impersonation or other electoral fraud? and
- iv. Did the procedures lead to an increase or a saving in expenditure?

The LGA compiled a brief summary of the responses from the above questions derived from the individual authorities' evaluation reports (refer to table 6).

**Table 6: Summary of 2000 Local Government Election Pilot Schemes**<sup>126</sup>

Question	Extended hours	Early voting	Mobile stations	Freepost	Weekend voting	Electronic voting & counting	Postal votes on demand	All postal ballots
i.	Marginally	Marginally	n/a	n/a	No	n/a	Sometimes	Yes
ii.	Yes	Yes	Yes	n/a	Yes	Yes	Yes	Yes
iii.	No	No	Decrease?	n/a	No	No	No positive evidence	No positive evidence
iv.	Increase	Increase-modest to heavy	Modest increase	Increase	Heavy increase	Increase-variable	Net increase	Heavy net increase

For a more in depth analysis the City of Salford (Salford) will be used as a case study. Salford was chosen because it was one of only three authorities that utilised electronic voting.

## Case Study: The City of Salford

### Background

Salford is a Metropolitan District, which in 2000 had 60 councillors representing 163,171 electors in 20 wards. As with all UK pilots, prior to any application being submitted to the Home Office for consideration, consultation with political party representatives must be undertaken to identify any possible objections. In the case of Salford no objections were identified. Approval for the pilot scheme was confirmed by issue of The City of Salford (Automated Voting and Counting Scheme) Order 2000. The electronic voting pilot scheme was conducted in the Irlam ward of the City, which in 2000 had an electorate of 7,324.<sup>127</sup>

Salford used touch-screen terminals, or DRE, in their pilot. The DRE was supplied by a consortium of two companies, a local company, Trilogy Information Systems Ltd. (TIS), and Global Election Systems Inc. (GES) of America. The system used was the Accuvote touch-screen electronic voting machine. The Accuvote touch-screen electronic voting machine was a similar model to the one evaluated in the Hopkins

<sup>126</sup> Table reproduced from Local Government Association. (2000). *Elections—the 21st century model—an evaluation of May 2000 local electoral pilots*. Research Report 14.

<sup>127</sup> Salford 2000.

Report discussed in chapter one. Additionally, GES Inc. was purchased by Diebold Inc. in 2001.

To facilitate electronic voting, four polling booths, each allocated with two voting machines, were situated within three polling places in Irlam. In addition, one presiding officer and poll clerk were allotted to each station together with a member of the TIS technical support team.<sup>128</sup>

## Preparation

Salford placed considerable emphasis on preparation and conducted inspections of the polling places being used in the pilot to identify potential problems; these were collaborative in nature and included TIS technicians. TIS conducted three training and familiarisation sessions for polling staff with the equipment and procedures that were to be used on election day. Electors were informed about the pilot scheme via media releases in the local newspapers. Electors were also invited to view and use the DRE in a mock election at the local library prior to the election.<sup>129</sup>

On the morning of the election, TIS delivered the DRE to the polling places. Polling staff prepared the DRE for operation. This involved inserting a disk in to the machine containing the necessary election data. TIS technical support was on hand in the event of problems being encountered, there were also spare machines available.<sup>130</sup>

'Readiness' tests were also conducted to ensure the machines were operating correctly, including the production of 'zero reports' to verify that the machines held no votes prior to the poll being opened. These reports were signed by the presiding officer and poll clerk and handed to the Deputy Returning Officer at the end of the polling period.<sup>131</sup>

## The voting process

Electors entered the polling place, confirmed their identity, were marked off the electoral roll and their elector identification number was relayed to a presiding officer. Electors inserted an 'elector card' into the voting machine to start the process and to display the candidate details. Candidate selection was made by touching the screen over the name of the preferred candidate.<sup>132</sup>

By touching the screen over the word 'next' electors could review their choice of candidate, and if necessary cancel their preference by touching it again. They made their alternative choice by touching the screen over their preferred candidate. Once satisfied, electors recorded their vote by touching the screen over the words 'cast ballot'. The DRE then recorded their vote and the elector card was removed from the voting machine and handed back to the presiding officer.<sup>133</sup>

At the close of the poll presiding officers accessed the machines by inserting an administration card and typing-in their personal identification number, enabling them to print a report of the votes cast for each candidate. The results were also downloaded from each machine onto a floppy disk. The printed report was attached to

---

<sup>128</sup> *ibid.*

<sup>129</sup> *ibid.*

<sup>130</sup> *ibid.*

<sup>131</sup> *ibid.*

<sup>132</sup> *ibid.*

<sup>133</sup> *ibid.*

the corresponding 'zero report' and along with the floppy disk delivered to the Deputy Returning Officer at the counting hall.<sup>134</sup>

## Counting of Votes

The electronic votes were sorted, counted and recorded on a summary sheet. Polling place presiding officers, upon arrival at the counting hall, handed over the floppy disk, the 'zero report', and the paper report of the votes cast for each candidate to the Deputy Returning Officer.<sup>135</sup>

A preliminary check of the 'zero report' was undertaken to verify that the machine commenced at zero votes and was signed by the presiding officer and poll clerk. Once satisfied, the total votes cast for each candidate were transferred to a summary sheet and together with the postal ballot paper count a final result was calculated manually and announced by the Deputy Returning Officer. At all stages of the count candidates and other interested parties were kept fully informed of proceedings and any queries were dealt with promptly.<sup>136</sup>

## Participation

The aggregate turnout in Irlam was 1,624 or 22 per cent (refer to table 7), with 1,577 ballots being electronically cast. Based upon these figures, 97 per cent of the ballots were electronic.

**Table 7: Irlam ward 2000 election turnout**<sup>137</sup>

<b>Irlam Ward</b>			<b>Electorate 7,324</b>
Elizabeth A Hill	Conservative	596	
Roger W Lightup	Labour	814	Elected
Julie Wenham	Liberal Democrat	214	
Turnout		22.17%	Total votes cast 1,624

Turnout in 2000, when compared with the 1999 turnout of 1,801, or 24.92 per cent, represents a 2.75 per cent fall in participation. In the authority as a whole turnout fell from 21.85 per cent in 1999, to 21.04 per cent in 2000. The fall in participation rates observed in Irlam was not a localised issue. There was considerable variance from ward to ward in the City and the fall in turnout observed in Irlam was not the highest. As noted in the Salford evaluation report, it is extremely doubtful that running the pilot was responsible for the fall as adjacent areas recorded similar falls.<sup>138</sup>

As stated earlier, Home Office circular RPA433 contained four questions that authorities were to use in the development of their evaluation reports. Salford conducted an exit survey to satisfy this requirement.

A total of 1,577 electronic ballots were cast, of this figure, 453 or 28.7 per cent, completed the questionnaire. Responses from the questionnaires are quite intuitive with only a small number, 17 per cent, regarding electronic voting as harder than the current system of completing paper ballots. Electronic voting, whilst considered easier to use than paper ballots, did not lead to a significant change in voting behaviour, with

<sup>134</sup> *ibid.*

<sup>135</sup> *ibid.*

<sup>136</sup> *ibid.*

<sup>137</sup> <http://www.salford.gov.uk/council/elections/results/resultsarchive/elections-2000.htm>

<sup>138</sup> *ibid.*

over 80 per cent of those surveyed stating that they vote every year regardless of what system is used. Only 3.5 per cent of respondents were motivated to vote by the introduction of electronic voting. Respondents were overwhelmingly satisfied with both the written and verbal instructions on how to use the electronic voting machines, at 74.2 per cent and 83.2 per cent respectively (refer to table 8).

**Table 8: City of Salford 2000 electronic voting pilot questionnaire responses<sup>139</sup>**

<b>The percentage of voters who found the electronic voting system</b>	<b>Reasons given for voting</b>
easier than the current system - 56.1%	vote every year - 83.2%
harder than the current system - 17.0%	appeal of electronic voting - 3.5%
the same as the current system - 26.9%	location of polling station - 2.7%
	interest in a party/individual - 9.1%
	other reasons- 1.5%
<b>Satisfaction level of written instructions (scale 1 poor/5 excellent)</b>	<b>Satisfaction level of verbal instructions given by polling staff (scale 1 poor/5excellent)</b>
1 6.8%	1 6.8%
2 3.5%	2 1.8%
3 15.5%	3 8.2%
4 25.4%	4 20.5%
5 48.8%	5 62.7%

As noted in the Salford evaluation report, electronic voting was widely accepted as a viable alternative to the current system of voting, and constructive comments flowed from the survey, particularly those relating to security.

Salford conducted a debriefing exercise involving polling staff, Elections Office staff and representatives from TIS. The central aim of this session was the identification of practical problems and suggested solutions (refer to Appendix 2). In general, polling staff were enthusiastic towards the concept of electronic voting and at being involved in an event of historical electoral importance. Staff indicated that the day was stressful on occasion, particularly when the machines were not functioning properly. Nevertheless, there was a general agreement the day was more interesting as there was greater interaction with electors than normal.

The success of the pilot is difficult to determine, or more precisely it depends on what criterion is used. One way to measure its success is the level of contestability of the result. Using this as the criterion then the pilot can be considered a success as ‘the political parties involved in the election ... appeared to be satisfied with the way the count was conducted and a result obtained [with] no evidence of any adverse reaction’.<sup>140</sup>

Salford sought feedback from political parties to ascertain their views on the pilot, in particular what the positives and negatives were from their perspective, opinions regarding the publicity campaign, impact on turnout and any other matters of relevance. The response was poor with only one respondent stating that the scheme should be tried again as long as the teething problems experienced were eliminated.<sup>141</sup>

<sup>139</sup> *ibid.*

<sup>140</sup> *ibid.*

<sup>141</sup> *ibid.*

Although the 2000 pilot was generally well received by the electorate, there were a few minor issues that resulted in thirteen paper ballots being issued. In one instance the voting machines were not working resulting in paper ballots being issued to electors who demanded their vote immediately; refusing to return later in the day to vote. In another, some electors had double pressed the screen on the voting machines causing it to 'jump' to the next screen, and because there was no return option were unable to 'jump' back and record their vote.<sup>142</sup> These issues can be considered minor in the context of the event; the first electronic voting trial in a local government authority.

## The 2002 pilot schemes

In 2002, there was a significant increase in the number and diversity of electronic pilots offered; nine authorities offered electronic voting, and 15 trialled electronic counting. Electronic voting could be conducted at a kiosk using DRE, over the Internet, via a standard touch-tone telephone, or via SMS text on a mobile telephone. A primary aim of the 2002 electronic voting pilots was to build public support and to establish security and reliability of the voting mechanisms, an aim which, according to the Commission, was achieved.<sup>143</sup>

A British National Opinion Poll (NOP) conducted in 2002, indicated a major obstacle to the introduction of electronic voting revolved around 'voter's reservations on the issue of security and fraud'.<sup>144</sup> The evaluations of the technology and processes used in the pilot schemes tend not to support these assertions. Great store was placed on protecting the integrity of the systems, with simulated 'hacking' exercises, restricted access to servers, and encryption technology utilised in the transmission of votes. These security precautions and others are discussed in greater depth below, using the Borough of Crewe & Nantwich as an example.

It is worth noting that despite these precautions a minority of electors who live in the local authorities that participated in the UK 2002 pilot schemes (both those who voted and those who did not), and participated in the Electoral Commission funded NOP survey expressed concern about security and fraud (figures reproduced below).

Electors and non-electors were less sure that the e-voting methods were safe from fraud or abuse. A majority in both cases thought the security measures were 'good' (62 per cent and 55 per cent), a minority 'poor' (17 per cent and 14 per cent), and a significant minority said that they did not know (15 per cent and 20 per cent) giving net scores of 45 per cent and 41 per cent respectively.<sup>145</sup>

However, the strategic evaluations conducted by the UK Electoral Commission after the 2002 pilot schemes revealed no evidence to suggest that the procedures or technology led to any increase in 'personation',<sup>146</sup> or any other electoral offences, or led to other malpractice in connection with the elections.<sup>147</sup> Therefore, it may be reasonable to assume that questions of security and fraud are more perceived than

---

<sup>142</sup> *ibid.*

<sup>143</sup> Electoral Commission 2002a.

<sup>144</sup> Xenakis and Macintosh 2004, p.60.

<sup>145</sup> Electoral Commission 2002d.

<sup>146</sup> Personation refers to someone pretending to be someone else.

<sup>147</sup> Electoral Commission 2002a, p.5.

real, and over time as electors become familiar with the technology the percentage of people with concerns may diminish.

The 2002 pilot schemes provide an opportunity to evaluate their experience in relation to security and fraud associated with Internet voting, and to provide an insight how such systems work.

### Case Study: Crewe and Nantwich Borough Council

Crewe and Nantwich Borough Council participated in the 2002 local election pilot schemes, and trialled internet voting in two wards, Maw Green and Wybunbury. These trials are particularly relevant in the context of this paper, as the Internet was the only electronic voting option offered in this pilot, allowing for a comparison to be made about the perceived threats discussed in chapter one against an actual event.

The project management for the pilot was conducted in partnership with two private corporations, British Telecom (BT) and Oracle, who together provided technical expertise. The council and its staff members supervised and coordinated the project and offered the following comments on the relationship:

The pilot was supervised by a Council Project Team chaired by the Assistant Chief Executive and comprising the Elections Manager and his line manager, the Press Officer, the Consultation Manager and the Internet Manager. The project plan, regularly updated, focused on the marketing aspects of the project rather than the technical aspects, which were managed largely by the BT/Oracle team in consultation with the Council's own IT experts. Oracle's Quality Management System ('QMS') project management methodology was used to run the trilateral project. As would be expected, this methodology included the requirement to have such things as a risk register, issues log etc. The Deputy Chief Executive kept very close to the project and provided hands-on leadership and support throughout (Electoral Commission 2002b, p.5).

The evaluation study regarding this particular pilot scheme indicated neither objection nor concern raised by the general public regarding the use of private organisations to assist in the technical aspects of the project. To further assess public satisfaction with the use of third parties in electoral affairs, an Internet archive search was conducted of the local *Crew Guardian* newspaper, where no negative results were reported.<sup>148</sup>

Electors in these wards were offered the opportunity to vote over the Internet, and to facilitate this, 16 digit Voter Identification Numbers (VIN) were posted out with voter's poll cards. To access the option of Internet voting a four digit PIN was also required, which was posted separately by the approved service provider BT.

During the four day Internet polling period electors voted by accessing a web site and by clicking the election button, choosing which ward they were entitled to vote in. Electors then entered their unique VIN and PIN numbers as part of the authentication process. These numbers were linked to the official electoral roll, and their activation did not reveal how one voted, only that a ballot was cast.

After keying the relevant information into the web site a ballot paper was produced, highlighting the candidates standing for election. Electors then 'clicked' their

---

<sup>148</sup> The archive search was conducted 23 May 2006, using search phrases 'e-voting' and 'elections'  
<http://archive.thisischeshire.co.uk>

candidate of choice, and were asked twice during this process to confirm that they had voted as intended. Electors could also cancel the vote and start again.

In relation to security and fraud, the following observations were made in the evaluation report, highlighting the security measures utilised to protect the integrity of the system. These included:

- The service provider, BT/Oracle, provided assurance that the system was as close as it was possible to get to being unbreakable, with seven layers of security;
- The use of VINs and PINs meant that all electors had valid entries on the electoral register and the data could be verified through the entire voting process;
- All voter information, including the vote itself, was encrypted with the decryption algorithms removed from the software. Root passwords to the Unix servers running the software and containing the vote details were known only by the Unix team within Oracle and the various teams had access only to their relevant part of the software;
- As part of BT's secure web hosting, there was continuous monitoring for intrusion of the system by outside sources. Physical access to the servers for the system was limited to a small number of staff, and required two swipe cards and a PIN number;
- The providers had used their own hackers – both internal and external – to identify any weaknesses. The layers of security were designed not only to screen out hacking but also to provide automatic switching in the event of equipment failure or Act of God; and
- On the personal security side, BT and Oracle staff were made aware of the importance of security, and the number of individuals able to access the system was small (limited to the development team and BT Oracle database administrators).<sup>149</sup>

Taken together the security measures adopted in this particular trial produced the desired result. That is, the election of representatives to the Borough Council that satisfied legal requirements under the relevant Act, with no recorded incidents of fraud or security breaches. In this context one could view the trial of internet voting as a success.

## Summary

As previously stated, a primary aim of the 2002 electronic voting pilots was to build public support and to establish security and reliability of the voting mechanisms. Security was achieved with the use of PIN and password codes, although, as the Commission noted, there was no standardisation and each authority in conjunction with their technology partner devised different formats.<sup>150</sup> In addition, whilst most

---

<sup>149</sup> Electoral Commission 2002b, p.5.

<sup>150</sup> Electoral Commission 2002a, p.43.

authorities had developed basic control mechanisms for their respective pilots, some failed to produce ‘security and testing documentation’.<sup>151</sup> The stated reason for this oversight was the absence of ‘slack’ built into the project plans, resulting in timetable pressures between project approvals and election-day.<sup>152</sup>

Nevertheless, and in the context of the security issues discussed in chapter one, there was no evidence to suggest the 2002 elections were subject to malicious attack or fraud. Furthermore, the Commission held talks with the relevant police forces in each pilot area to ascertain if there were any acts of electoral fraud. There was only one such act, in Stratford on Avon, and ‘the nature of the fraud [did] not relate to the pilot scheme itself’.<sup>153</sup> In comparison, the postal ballot pilots proved to be more controversial with a number of ‘fraud scares’ being reported; but as the Commission noted, there were no substantiated allegations of fraud, and ‘out of 144,052 electors only 171 ... applied and were re-issued with ballot papers’.<sup>154</sup>

Actual voting data from the 2002 trials reveal that of the 28 wards which conducted electronic pilots, nearly 25 per cent of votes cast were electronic; with the Internet proving to be the most popular (refer to table 9). Although this is a crude measure to gauge public support it does provide a valuable insight, and given that the average turnout across all local authorities in 2002 was low at 32.8 per cent,<sup>155</sup> and approximately 50 per cent of the British population had access to the Internet, either at home or work,<sup>156</sup> the figures are encouraging. According to UK research, 63 per cent of the British population will have access to the Internet by 2005,<sup>157</sup> and if voting was compulsory, the convenience of electronic voting, in particular the Internet, might produce a dramatic increase in the number of electors using new voting technologies.

**Table 9: Multi-channel pilot schemes turnout**<sup>158</sup>

Authority & number of wards	Attendance/ Postal		Internet		Telephone		SMS Text	
	n	%	n	%	n	%	n	%
Crewe 2	1,839	83.5%	364	16.5%	–	–	–	–
Liverpool 2	3,957	59.4%	1,090	16.4%	1,162	17.4%	445	6.7%
St Albans 2	1,539	49.5%	825	26.5%	744	23.9%	–	–
Sheffield 3	8,881	67.7%	2,904	22.1%	–	–	1,327	10.1%
Swindon 19	33,329	84.1%	4,293	10.8%	2,028	5.1%	–	–
<b>Total 28 wards</b>	<b>49,545</b>	<b>76.5%</b>	<b>9,479</b>	<b>14.6%</b>	<b>3,934</b>	<b>6.1%</b>	<b>1,772</b>	<b>2.7%</b>

The Commission recognises that if public concern about security and fraud was to grow it might undermine confidence in new voting technology and future pilot programs. With that in mind the Commission sees it as essential to establish criteria against which future pilots can be assessed. For the 2002 pilots there was no such criterion in place to assess potential suppliers of technical services or to evaluate the pilots once operational. However, the Commission did take into consideration ‘e-specific criteria’ developed in other jurisdictions; California, the UK Independent

<sup>151</sup> *ibid*, p.42.

<sup>152</sup> *ibid*.

<sup>153</sup> *ibid*, p.69.

<sup>154</sup> *ibid*, pp.35–36.

<sup>155</sup> *ibid*, p.61.

<sup>156</sup> *ibid*, p.17.

<sup>157</sup> *ibid*.

<sup>158</sup> *ibid*, p.44.

Commission on Alternative Voting Methods, and the technical committee of the international Organization for the Advancement of Structured Information Standards (OASIS) group.<sup>159</sup>

## The 2003 pilot schemes

In 2003 a particular emphasis was placed on remote electronic voting via the Internet and 59 authorities participated, 17 offered electronic voting and 14 offered remote electronic voting. In all, 160,000 electors cast an electronic ballot in the May 2003 pilot schemes.<sup>160</sup>

As was the case in 2002, the option of using the Internet was the most popular channel offered. The process to cast an electronic vote over the Internet was similar to that used in previous years. Electors logged onto the election website either directly or via the local authority website. The relevant information and web addresses were delivered with the elector's poll card. The process for Internet voting is described below:

- Electors logged onto the system using the 'credentials' provided on their poll card. There was no standardisation in the way the 'credentials' were supplied, with some authorities using two mailings to deliver the information (Kerrier, Sheffield, Shrewsbury & Atcham and Vale Royal), with the rest using one mailing.
- Candidate selection was made by 'clicking' on the ballot screen with the mouse, or by typing in the candidate number. Interestingly, an elector could cast a blank vote by not choosing any candidates, although this information was generally not promoted.
- Upon making a selection the screen displayed the candidate or candidates that the voter had selected, or in the case of a 'blank vote', informed the elector that no choice had been made. The elector could then either confirm their selection, or go back and change it.
- In some instances the system displayed a confirmation that the voting process had been completed. In Ipswich, Norwich, St Albans, South Somerset and Sheffield, a receipt ID was given which could be compared with the corresponding receipt ID on the poll card. In Stratford on Avon a receipt was given that the voter could use at a subsequent web page to confirm that his or her vote had reached the ballot box.<sup>161</sup>

As previously stated, authorities took different approaches to providing electors 'credentials'. They also used different terminology and character lengths. Typically, 'credentials' consisted of two separate parts, a VIN and PIN. For example, 'Kerrier used Part 1 of the PIN (which was visible on data entry like a computer username) and Part 2 of a PIN (which was invisible like a computer password), [Stratford used]

---

<sup>159</sup> *ibid*, p.49.

<sup>160</sup> Electoral Commission 2003a, p.49.

<sup>161</sup> *ibid*, p.51.

an additional ballot code alongside the VIN and PIN; [where as] Swindon and Stroud used a two-part ballot code'.<sup>162</sup>

The lack of commonality in the terminology used by technology suppliers and the relevant authority sometimes resulted in different terminology appearing in separate items of voter literature. It was noted that '...South Tyneside, used different credentials, with different lengths, for each of the three channels provided (an eight-digit user ID number and eight-digit password for the internet channel, a six-digit user identity number and eight-digit password for the touchtone telephone channel, and a 12-digit access code for the text message channel)'.<sup>163</sup> Additionally it was noted that in authorities offering multiple voting channels the provision of 'multiple credentials' makes explaining the voting process complex and has the potential to confuse electors with no obvious benefits.<sup>164</sup>

Of the 17 authorities that offered electronic voting only two reported significant operational problems, St Albans and Sheffield. According to the Electoral Commission the problems were resolved satisfactorily. In both of these authorities electors could vote in person at a polling place as well as voting remotely by Internet, Telephone, and in the case of Sheffield by text message, right up to the close of the poll. To prevent multiple voting, one of the concerns discussed in chapter one, the process of applying for a ballot at a polling place was changed and included the use of an online register that was updated in 'real time' every time a valid vote was placed. This was achieved with the use of PCs at the polling place connected to the 'central voting platform' over the Internet.<sup>165</sup>

The above mentioned problems occurred due to the late delivery and setup of the required PCs, resulting in the majority of polling places in the two pilot areas being un-operational when the polls opened on election-day. Subcontractors supplying the PCs on behalf of authority's technology partners BT, were responsible for the late delivery and installation. The Electoral Commission contended that the requirement of 'online connectivity to a large number of polling stations with varying facilities is not an easy task [and] careful attention should be paid to risk management in this area'.<sup>166</sup>

The Electoral Commission noted the efforts of the St Albans Returning officer and the election team in managing the problem. This was the second time that they had conducted an electronic pilot, the first was in 2002, and may help explain their preparedness. Each polling place was provided with a backup manual copy of the voting register indicating who had voted prior to the start of the traditional election day. This allowed people to vote and no one was intentionally turned away, even though there was a risk that some electors could have voted twice. Following the close of the poll the Returning Officer conducted a verification audit with the intention of removing any duplicate ballots. Although it was not made explicitly clear one assumes that in the event of a duplicate ballot being found, that it would be the electronic ballot that would be excluded from the count. There were, according to the Electoral Commission, no duplicate votes identified and the count commenced three

---

<sup>162</sup> *ibid.*

<sup>163</sup> *ibid.*

<sup>164</sup> *ibid.*

<sup>165</sup> *ibid.*, p.56.

<sup>166</sup> *ibid.*

hours after the close of the poll. Political parties were informed of the problems and at no point did they 'raise any serious queries relating to the count'.<sup>167</sup>

In relation to the threats discussed in chapter one, the Electoral Commission, in conjunction with the UK Government's Communications-Electronics Security Group (CESG), conducted a security analysis to inform pilot participants about potential threats and solutions associated with electronic voting. The premise was that no trust could be placed on the client's system (an elector's computer or mobile phone) and the use of randomly generated 128-bit pre-encrypted ballots was recommended.<sup>168</sup>

In 2003, due to the increase in the number of remote electronic voting channels and postal ballots, an emphasis was placed on monitoring for acts of coercion and vote selling. The Electoral Commission in partnership with the Crown Prosecution Service (CPS) developed and promoted mechanisms for reporting allegations of electoral fraud in the pilot areas. There was also a statutory requirement on Returning Officers to report any allegations of fraud to the Commission. No acts of alleged fraud were recorded either directly to the CPS or individual Returning Officers. In addition a number of authorities conducted fraud checks. None of the checks uncovered acts of fraudulent voting.<sup>169</sup>

There were however attempted acts of 'double-voting' recorded in some pilot areas, but these incidents did not represent fraudulent acts. Instead the problem was sourced back to a text message confirmation failure. There was also an incident, or alert, reported to the 'Government's Computer Emergency Response Team' during the election period; on investigation it turned out to be a false alarm as it was actually security testing being conducted on the systems by the Government's own Quality Assurance contractors.<sup>170</sup>

Analysis of the voting systems log files reveal 'attempted and actual security attacks' being recorded; investigations revealed the attacks were 'regular probing attacks undertaken by automatic hacking programs on the web'.<sup>171</sup> It was the view of the Electoral Commission that the 'level of Internet noise [was] common and [did] not represent targeted attacks on the e-voting services'.<sup>172</sup>

## **Case Study: St Albans City and District Council**

St Albans was granted permission to conduct electoral pilots in the 1 May 2003 local government elections. There was a diverse range of voting channels offered to electors; touch-tone telephone, Internet and electronic voting at polling places using DRE.

In 2003, St Albans had a population of approximately 129,000; of this number approximately 97,000 were registered to vote. St Albans can be viewed as an affluent area with an educated population. Survey data compiled in 2002 indicated that 86 per cent of the population had access to the Internet.<sup>173</sup>

---

<sup>167</sup> *ibid.*

<sup>168</sup> *ibid.*, p.57.

<sup>169</sup> *ibid.*, p.61.

<sup>170</sup> *ibid.*

<sup>171</sup> *ibid.*

<sup>172</sup> *ibid.*

<sup>173</sup> Electoral Commission 2003b, p.4.

## Voting period

Electronic voting was conducted from 9am Monday 28 April until 9am Thursday 1 May 2003. Attendance voting using either a paper ballot or DRE was conducted between 8am and 9pm on election-day 1 May 2003. As a security measure to prevent double voting an online electoral register was used at polling places. When electors entered they were marked off and the register was updated in 'real time'. This was necessary because electors could cast an electronic ballot up until 9am on election-day.<sup>174</sup>

## Security and Authentication

Voting electronically required a unique personal 'Voter ID' number and password for the validation process. These numbers were supplied on the elector's poll card and were hand delivered by election staff. The four digit password was protected by security foil to attest that it had not been compromised.<sup>175</sup> It is worth noting the St Albans pilot did not make the mistake of confusing electors or over complicating the process by using different credential configurations.

A major concern discussed in chapter one was the lack of an electronic audit trail. In St Albans, electors who cast an electronic ballot were provided with a unique receipt number linked to their voter ID. This measure was intended to reassure electors that their vote had been registered and provided a means to refer back to the Council if necessary.<sup>176</sup> Additionally, as a safeguard against malicious 'insider attacks', all the 2003 UK pilots had the capacity to trace electronic ballots to the elector.<sup>177</sup>

The ability to trace votes is a technical security requirement and forms part of the CESG security solution. CESG states 'that votes must be anonymous but traceable (in the event of a court order) and that there must be confidentiality in transmission through the use of techniques such as end-to-end encryption.'<sup>178</sup> This requirement of traceability allows the Electoral Commission to obtain a court order to verify election results in the case of alleged fraud and acts as a deterrent to would-be fraudsters.

## Electors feedback

In St Albans public awareness of the voting pilots was accomplished via multiple means and can be considered consistent with other local authorities in previous years. In order to ascertain electors' thoughts and perceptions on electronic voting, all electors who cast a remote electronic ballot were asked to participate in an 'optional' post-voting questionnaire (refer table 10).

---

<sup>174</sup> *ibid.*

<sup>175</sup> *ibid.*

<sup>176</sup> *ibid.*, p.6.

<sup>177</sup> Electoral Commission 2003a, p.108.

<sup>178</sup> *ibid.*, p.107.

**Table 10: Post voting questionnaire results summary**<sup>179</sup>

<b>Telephone voting (3,718 responses)</b>	<b>Internet voting (7,490 responses)</b>
84% found it easy to use	80% used their home computer to vote
2.5% found it very difficult to use	19% voted at work
95% would use it again	1% voted at another location
3.6% might use it again	98% would vote over the internet again
1.5% would not use it again	2% might use the internet again
17% said that they would not have voted if the facility had not been available	a negligible amount would not use the internet again
20% felt that they were only given limited information	98% found the screens and instructions either very clear or fairly clear
57% of users were female	9% felt that they were only given limited information
	45% of voters were female

### Logistical and support issues concerning polling stations

St Albans experienced problems in preparing polling places in time for the opening of the poll, with only 11 per cent of polling stations being electronically operational by 8am. A further 41 per cent had equipment installed but not operational, 43 per cent had equipment delivered but not installed, and 5 per cent did not have any equipment at all. The problem was attributed to outsourcing problems associated with the supply of the computers required to manage the electronic electoral roll.<sup>180</sup>

St Albans received an installation schedule from BT on 24 April, with a further update on the 28<sup>th</sup> and raised concerns regarding timelines and resources given the short period outlined in the schedule. St Albans was informed that the installation was proceeding to schedule, but at least 25 polling stations remained uninstalled by the end of 30 April, and the majority of polling stations were not functioning electronically at 8am on 1 May.<sup>181</sup>

### Issues with touch screen kiosk voting at polling stations

Inspections of the polling places revealed that most of the touch screen kiosks were not working, and those that worked were subject to periodic crashes. There was a concern the crashes and subsequent error messages confused some voters and may have potentially undermined their confidence in the integrity of the electronic voting process.<sup>182</sup>

In addition, the following observations were made:

- individuals found the touch screen technology unresponsive or difficult to use;
- those unfamiliar with PCs being confused by the Hourglass symbol;
- voters not knowing how to work the poll card barcode scanners;
- the provision of computer chairs on wheels in polling stations with polished and or wooden floors was a potential health and safety issue.<sup>183</sup>

<sup>179</sup> *ibid*, p.13.

<sup>180</sup> *ibid*, p.17.

<sup>181</sup> *ibid*.

<sup>182</sup> *ibid*.

<sup>183</sup> *ibid*.

## Issues with the online electronic register at polling stations

A notable issue recognised by St Albans and BT was the periodic crashing and performance degradation of the online electoral roll, which on occasion denied election staff access to information on who had voted. A possible future solution considered by St Albans and BT, in acknowledgment that Internet Service Providers (ISP) do not guarantee the performance element of the Internet, was the creation of a dedicated fixed connection, or creating their own ISP. However, such a move would require greater resources and time.<sup>184</sup>

## Issues with internet browser requirements

A significant oversight reported by electors was the need to have access to an internet browser that supported 128-bit encryption. The issue was overcome by advising electors (who experienced this problem) to download the required application from the Internet. St Albans was assured by BT that they responded promptly to the issue by advising their helpdesk and providing a work-around in the form of a download.<sup>185</sup>

## Impact on turnout

St Albans provides an interesting insight into electoral behaviour, particularly the potential for electronic voting making the democratic process more accessible, convenient, and increasing turnout. Using 2000 as a baseline, the last time a conventional election was conducted, a picture can be developed on electoral participation (refer table 11).

**Table 11: St Albans election turnout 2000–2003<sup>186</sup>**

2000	2002	2003
Conventional	1 <sup>st</sup> voting pilot schemes	2 <sup>nd</sup> voting pilot schemes
34%	38%	43.3%

The increase in participation suggests that the St Albans electorate are willing to accept the perceived security threats associated with electronic voting, and may well be willing to trade off the perceived security associated with conventional elections for more choice and convenience. As the St Alban's evaluation report notes; there were no 'significant local issues' in 2003 to galvanise the minds of electors and influence turnout, and that 40 per cent of those who voted chose to do so electronically (refer table 12). Furthermore, the St Albans evaluation report suggested that the availability of electronic voting could have contributed to the increased turnout; but most certainly increased the choice and flexibility of voting methods available to the public.<sup>187</sup>

---

<sup>184</sup> *ibid*, p.18.

<sup>185</sup> *ibid*.

<sup>186</sup> *ibid*, p.19.

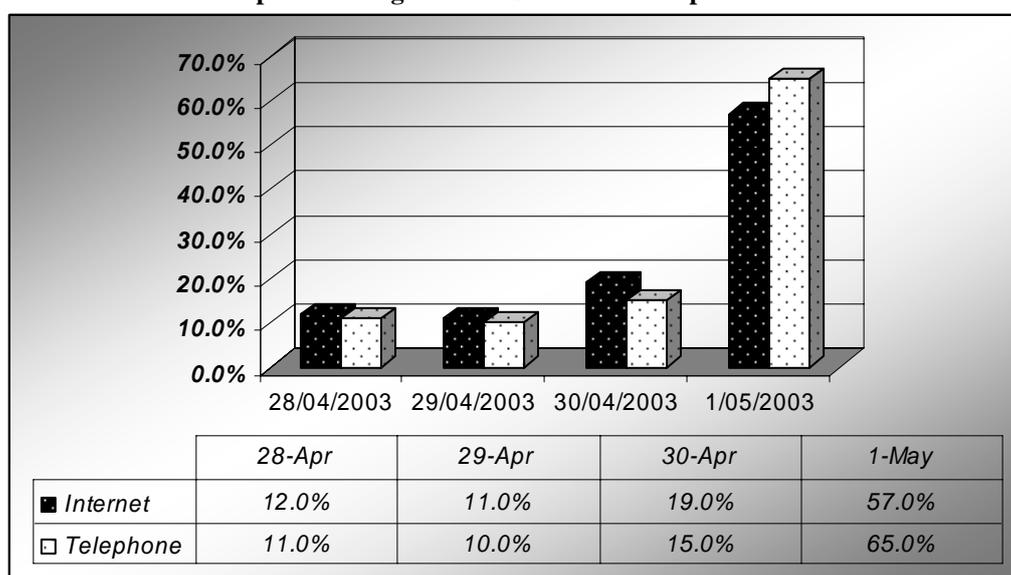
<sup>187</sup> *ibid*.

**Table 12: Breakdown of the different channels used in the St Albans 2003<sup>188</sup>**

Voting Method	Participation Rate
Paper ballots cast at polling station	39.3%
Postal ballots	19.3%
Internet voting	24.4%
Kiosks (community and polling stations)	5.2%
Telephone	11.8%

An analysis of the 2003 election data reveals the following voting patterns, 57 per cent of internet voting took place on 1 May 2003 (the traditional polling day), even though voting channels were available from 28 April until 1 May. The data for telephone voting follows a similar trajectory to Internet voting, with 65 per cent of telephone voting taking place on 1 May (Refer chart 5).

**Chart 5: Internet and telephone voting volumes St Albans 2003 pilot<sup>189</sup>**



The third channel for electronic voting, kiosk voting, produced limited data with only 12 ballots being cast over the three day voting period. The majority of kiosk voting took place on 1 May, with 2,736 ballots being cast. According to the St Albans' evaluation report, the extremely low volumes of kiosk usage may be attributed in part to their availability in only four community locations, and given the low participation rates may have reflected attitudes to voting in public locations.<sup>190</sup>

<sup>188</sup> *ibid.*  
<sup>189</sup> *ibid.*, p.20.  
<sup>190</sup> *ibid.*

## Chapter Six: The Australian Experience: EVACS

Australia has been relatively slow in developing electronic voting systems, although computers have been a fundamental part of the electoral system for many years; in particular, the management of electoral rolls, counting of ballots, and distributing preferences. At the federal level there has been no trial of electronic voting to date, while at the state and territory level only the Australian Capital Territory (ACT) has conducted an electronic voting trial (twice).<sup>191</sup> This chapter focuses on the ACT Legislative Assembly Elections of 2001 and 2004, where an 'Electronic Voting and Counting System' (EVACS) was developed and utilised.

### Background to EVACS and the 2001 trial

The catalyst for the ACT trial stems back to the 1998 Legislative Assembly Election, where a close result in the Molonglo electorate necessitated a recount. Two candidates were separated by three votes and a recount revealed an error in the initial manual counting process, resulting in calls for an automated system to increase the speed and accuracy of the election system. A prerequisite for the trial was a change to the *Electoral Act 1992* to allow electronic voting. On 5 December 2000 the *Electoral (Amendment) Act 2000 (No 2)* was passed by the Legislative Assembly, paving the way for the trial to begin.<sup>192</sup>

Following the passing of the necessary legislation tenders were called to supply the software, resulting in seven responses, with Software Improvements Pty Ltd being announced as the successful tenderer on 19 April 2001.

During the development stage consultation was undertaken with Members of the Legislative Assembly (MLAs) and political party representatives on the design of the electronic voting system, with a particular emphasis placed on the voting interface. Additionally, a Reference Group was established consisting of MLAs, representatives from political parties, special interest groups, ACT Blind Citizens Australia, and the Proportional Representation Society. The group was consulted on the design of EVACS and provided feedback on its development.<sup>193</sup>

### Testing and auditing of EVACS

According to the ACT Electoral Commission, EVACS was extensively tested prior to its implementation to ensure the system accurately counted votes and distributed preferences under the ACT Hare-Clark voting system. The testing was informed by a series of documents developed by the Commission that stipulated the software requirement specifications, design specifications, acceptance test plans, and procedure specifications. The documents were developed to appropriate industry standards, particularly the Institute of Electrical and Electronics Engineers (IEEE) standards 829-1998<sup>194</sup> and 830-1998<sup>195</sup>. These documents informed the testing team and the testing methods employed, and covered the following aspects of EVACS:

---

<sup>191</sup> There is speculation that the next federal election in 2007 will trial some form of electronic voting.

<sup>192</sup> ACT Electoral Commission 2002, p.6.

<sup>193</sup> *ibid*, pp.6-7.

<sup>194</sup> IEEE 829-1998 standard for software test documentation.

<sup>195</sup> IEEE 830-1998 recommended practice for software requirements specifications.

- Conducting structured test cases in controlled situations (used to ensure individual modules perform as expected);
- Conducting Hare–Clark scrutinies in parallel, using EVACS and manual counting of known sets of ballot papers, comparing the results obtained by EVACS and the Commission’s Excel spreadsheet Hare–Clark program (used to ensure that EVACS was correctly applying the Hare–Clark system, using a variety of test election outcomes to test specific cases);
- “Real user” testing, whereby large number of users cast electronic votes in a mock polling place and data–entry operators entered the results from paper ballots (used to test useability and to simulate realistic loads on the system);
- Load testing, where large quantities of ballot data was simulated and loaded into the counting system; and
- “Whole of life” testing where the entire process was simulated, taking test electronic votes from a polling place, loading it into the counting server, adding data-entered results from paper ballots, and using the counting system to generate a Hare–Clark result.<sup>196</sup>

In addition, EVACS was audited to ensure no ‘malicious code’ had been embedded into the software for the purpose of altering the election result, or changing or substituting ballots. The auditors certified the source code of EVACS capable of the following:

- Appeared to neither gain nor lose votes;
- Appeared to faithfully implement the Hare–Clark algorithm for vote counting provided to BMM by the Commission; and
- Was written in a consistent, structured and maintainable style.<sup>197</sup>

## The electronic voting system

In 2001 the option of casting an electronic ballot was made available in two ways, at one of the four pre-poll voting locations<sup>198</sup> or at one of eight polling-place locations on election day.<sup>199</sup> The system was based on the use of standard PCs configured to be used as voting terminals. Each PC had a barcode reader attached, allowing electors to activate the system and cast a ballot. Each PC was linked to a dedicated server located at each polling-place communicating over a secure local area network. The EVACS system did not receive any votes or transmit any data over a public network such as the Internet.<sup>200</sup> In contrast the 2004 trial utilised a limited amount (14) purpose built voting tablets, in conjunction with the PC model used in 2001, which were proved to be a robust and more portable alternative to the conventional PC.<sup>201</sup>

## Security

Security of EVACS was achieved through the use of barcodes, coded with a unique number linked to a particular electorate and polling-place. To prevent barcodes from being forged, or the production of ‘homebrew’ imitations, each barcode was digitally signed. The barcode number was converted into another number, referred to as a hash. When an elector was given a barcode for the purpose of casting a ballot, the server

<sup>196</sup> ACT Electoral Commission 2002, p.7.

<sup>197</sup> *ibid*, p.8.

<sup>198</sup> Belconnen, Canberra City, Tuggeranong, and Woden.

<sup>199</sup> Belconnen, Canberra City, Tuggeranong, Woden, Gungahlin, Melba, Richardson, and Weston.

<sup>200</sup> ACT Electoral Commission 2002, p.8.

<sup>201</sup> ACT Electoral Commission 2005, p.3.

matched it to the corresponding hash number for the purpose of establishing the barcodes uniqueness and to verify that the barcode has not been previously used.<sup>202</sup>

## Casting a ballot

Although the option of casting an electronic ballot represented a fundamental change compared to previous elections, electors in Canberra would have been familiar with certain aspects of the process. Electors attended a polling-place as per normal, got directed to an issuing officer for the purpose of establishing their entitlement to vote, and if eligible, were offered the opportunity to cast an electronic ballot. There was no compulsion; electors were free to choose to vote either electronically or traditionally with a paper ballot. If the electronic option was chosen, electors were issued with a barcode and directed towards a PC.<sup>203</sup>

Electors started the process by choosing their preferred language, there were 12 pre-programmed, with English being the default. In the advent of a non-English language being chosen, all screen images used that language with English subtitles displayed underneath. Once the preferred language was determined electors swiped their barcode through the barcode reader, if the barcode was read successfully an audible 'beep' was heard and a ballot was displayed on the screen.

The Commission concedes there were a few issues with the bar code readers, describing them as 'temperamental' and failing to read the barcode on the initial swipe, often requiring multiple attempts to activate the system. On occasion the barcode would trigger an error message to be displayed on the screen instructing electors to seek assistance from polling staff. The error message contained a number indicating to the polling staff the nature of the problem. Typically the error number related to one of the following:

- The barcode was not for that polling-place;
- The barcode had been used before; or
- The barcode was not valid for that election.<sup>204</sup>

In these instances polling officials would reset the PC to the welcome screen by entering a 'keyboard combination' and inviting the elector to try again. If the nature of the error message warranted further investigation, or the PC would still not recognise the barcode, a polling official would manually enter the barcode number into the server PC to establish whether or not the system recognised it, or whether there was a record of previous use. In the event these investigations indicated that the barcode had been used, and the elector maintained they had not used it, then a declaration ballot was issued to enable the elector to cast a vote. The declaration ballot and the barcode were then quarantined for later determination by the Electoral Commissioner, and if the computer records indicated a successful ballot had been cast the declaration vote would be declared invalid. Alternatively, if the investigation revealed that the barcode had not been used, or that the system could not read it, the elector was issued with another barcode.<sup>205</sup>

---

<sup>202</sup> ACT Electoral Commission 2002, p.29.

<sup>203</sup> *ibid*, p.30.

<sup>204</sup> *ibid*, pp.30-31.

<sup>205</sup> *ibid*, p.31.

In recognition of the ‘temperamental’ nature of the barcodes enhancements were made for 2004 trial. In particular measures were taken to ensure that the size and font of the barcode was compatible with all the barcode readers used by the Commission. This measure was generally successful in eliminating the need for electors to make multiple swipes to activate the system to cast a ballot. The change was received well by electors frustrated by the process in 2001, and generally sped up the voting process.<sup>206</sup>

### How the system fared

The Commission contended that in 2001, notwithstanding the temperamental nature of the barcodes, the system was well received by electors. Accuracy concerns were raised publicly but the Commission maintained that the testing regime, combined with established electoral processes, meant ‘the system was close to 100 per cent accurate and these concerns were unfounded’.<sup>207</sup>

In 2001 a total of 16,559 electronic votes were recorded. The system eliminated the need for manual counts, thus reducing the potential for errors, and the whole process of counting was accelerated. Additionally, the system was successful in reducing unintentional elector errors and informal votes.<sup>208</sup> In contrast the 2004 trial, whilst providing the same benefits described above, realised a marked increase in the number of electronic votes cast: 28,169, which represents a 70 per cent increase on the 2001 figure. In totality, 13.4 per cent of all votes counted in 2004 were electronically cast compared to 8.3 per cent in 2001.<sup>209</sup>

### Pre-polling Centres

At the four pre-poll centres used in 2001 a total of 21,739 ballots were cast over the period 02 Oct–19 Oct, with 52.4 per cent of the votes being electronic. The Woden pre-poll centre received the highest number of electronic votes, with 76.8 per cent of all votes cast being electronic. In contrast the Canberra City pre-polling centre received the lowest percentage of electronic votes, 38.1 per cent, with Belconnen and Tuggeranong recording 53.3 per cent and 45.8 per cent respectively.<sup>210</sup>

The Commission surmises that the variation in the number of electronic votes between the pre-polling centres can, to some extent, be attributed to the confidence of the staff involved and periods of high demand. In the case of Woden, polling staff were more familiar with the system and its functionality as this site was used in pre-election trials; consequently, they were better placed to promote the benefits to electors. Conversely, the City location received most of its votes during the lunch period, creating operational pressures as all ten electronic booths were constantly occupied at these times, necessitating the need to distribute paper ballots to ease the build-up of queues.<sup>211</sup>

On occasions some of the systems froze and had to be re-booted. Electors affected by such instances were issued with paper ballots. The Commission contended that no votes were lost due to computer failures, nor were there any major down times.

---

<sup>206</sup> ACT Electoral Commission 2005, p.8.

<sup>207</sup> ACT Electoral Commission 2002, p.2.

<sup>208</sup> *ibid*, p.1.

<sup>209</sup> ACT Electoral Commission 2005, p.3.

<sup>210</sup> ACT Electoral Commission 2002, pp.9, 38.

<sup>211</sup> *ibid*, p.9.

Further, the use of EVACS at pre-polling centres reduced the scrutiny workload by approximately 50 per cent.<sup>212</sup>

In contrast the 2004 trial realised an increase in the total number of electronic votes cast during the pre-poll period, from 52 per cent in 2001 to 68 per cent. The Tuggeranong pre-poll centre issued the largest number of electronic votes, 5,657, which represents 78 per cent of all votes cast at that pre-poll centre. The Tuggeranong experience is quite insightful, in 2001 only 45.8 per cent of votes cast were electronic and the increase in 2004 might signal a growing acceptance in the electorate of both the technology and security of EVACS. Even the Canberra pre-poll centre realised an increase in the number of electronic votes cast. In 2001 electronic votes represented 38 per cent of all votes cast compared to 59 per cent in 2004. The Commission contended that there were no major 'down times' recorded at any of the 2004 pre-polling centres; although, the Tuggeranong pre-poll centre ran out of barcodes due to high demand on the last day of the pre-polling period.<sup>213</sup> One may surmise that had there been a sufficient number of barcodes for all those who wished to cast an electronic vote then may be Tuggeranong might have breached the 80 per cent mark.

### Electronic voting on polling day

In 2001 eight locations were established to offer electronic voting; the four pre-polling centres and four additions. The preparation of the four additional locations caused a few problems, mainly access, as they were not available until the Friday prior to the election day resulting in preparation constraints. Of the four additional polling places, only Weston and Melba experienced problems, whilst Gungahlin and Richardson were incident free.<sup>214</sup>

The commencement of electronic voting was delayed at the Weston polling-place due to the failure of a 'set up disk', and the administration server 'froze' on occasion resulting in the need to reboot the system. Eventually, after a number of freezing episodes electronic voting was abandoned later in the day.<sup>215</sup>

A server failure at the Melba polling-place resulted in the loss of electronic voting for approximately half an hour whilst a replacement was installed. The Commission asserts that the server failure did not result in any 'lost votes' because all election data was stored on recoverable 'mirrored hard disks' and that the fail safes built into the system were reliable and worked well.<sup>216</sup>

In 2004 the same formula was followed, the four pre-polling centres were used on election day along with four additional centres. Once again problems of access to the additional locations caused preparation constraints, although the setup procedures and installation of hardware was completed on time. Unlike 2001 where server failures and setup delays were experienced the 2004 trial was trouble free and no difficulties were experienced during the polling day.<sup>217</sup>

---

<sup>212</sup> *ibid.*

<sup>213</sup> ACT Electoral Commission 2005, p.12.

<sup>214</sup> ACT Electoral Commission 2002, pp.9-10

<sup>215</sup> *ibid.*, p.10

<sup>216</sup> *Ibid.*

<sup>217</sup> ACT Electoral Commission 2005, p.13.

## From the electors' perspective

Exit polls were conducted in 2001 and 2004 to gauge the opinion of those who cast an electronic ballot. The reader should be aware that the sample sizes were quite low, 295 respondents in 2001 and 54 in 2004, and as a consequence inferences should be made with caution. Nevertheless, the data provides an insight into electors' perceptions of electronic voting (refer table 13).

**Table 13: Electors perspective on EVACS**

	2001 <sup>218</sup>	2004 <sup>219</sup>
Ease of use		
➤ Easy	89 %	86 %
➤ Not easy	11 %	14 %
Clarity of instructions		
➤ Clear	81 %	83 %
➤ Not clear	15 %	N/A
➤ Unsure	4 %	N/A
Timeliness		
➤ Fast & efficient	70 %	88%
➤ Not fast & efficient	21 %	N/A
➤ Unsure	9%	N/A

The data indicates that EVACS is a simple voting technology to use with both 2001 and 2004 respondents expressing a high rate of ease of use and a similarly high response in relation to clarity of instructions. There also appears to be a marked increase in the level of satisfaction associated with speed and efficiency in casting a vote. Unfortunately the Commission's report on the 2004 trial did not contain data on the level of dissatisfaction/unsureness as was the case in 2001.

In both 2001 and 2004 there were a small number of complaints (less than ten on both occasions). In 2001 some electors alerted officials to finding 'open ballots' on the terminal screens, indicating the previous elector did not complete the ballot process. The Commission acknowledges that this was unfortunate and ultimately led to disenfranchisement for those individuals as their ballots was classed as informal and excluded from the count. For electors finding open ballots it was not possible for them to complete the process and vote twice, as EVACS requires the same barcode to start and complete the process.<sup>220</sup>

In 2004 as was the case in 2001, some electors asserted that they had unintentionally voted informally. The Commission argues (on both occasions) that it is not possible to unintentionally vote informally because it would require an elector to activate the finish key without selecting a candidate and swiping the barcode a second time to finish the process. In addition such actions would also be carried out whilst ignoring a prominent message stating 'if you swipe your barcode now your vote will be informal'.<sup>221</sup>

<sup>218</sup> ACT Electoral Commission 2002, p.10

<sup>219</sup> ACT Electoral Commission 2005, p.14.

<sup>220</sup> ACT Electoral Commission 2002, p.10

<sup>221</sup> ACT Electoral Commission 2002, p.10 & ACT Electoral Commission 2005, p.14.

## The elimination of unintentional voting errors

Perhaps one of the most encouraging aspects of EVACS is the potential to eliminate unintentional voting errors. This is accomplished through automatic numbering of candidates as they are selected by an elector. Once an elector makes their first candidate choice the computer program automatically marks that preference as one (1) in the candidate square and subsequent choices are marked sequentially thereafter until all choices are exhausted.<sup>222</sup>

This measure, automatic preference numbering, proved a useful tool during the 2001 general election in protecting a citizen's democratic right to vote. Especially when compared against the number of informal votes that there was recorded by those who voted in the traditional manner using a paper ballot. The error rate recorded, for those who voted but mistakenly completed the ballot paper is quite telling. In all there were 2,866 ballot papers incorrectly marked and consequently excluded from the end result. A further analysis of the data reveals that 1,141 electors incorrectly sequenced their preferences (1,2,4,5 as oppose to 1,2,3,4) and 1,725 electors repeated a number (1,2,3,4,4, as oppose to 1,2,3,4,5).<sup>223</sup> As the ACT electoral commission notes, it is hard to determine the level of deliberate ballot spoiling but it would not be unreasonable to assume that those electors who wished to make such a protest would simply not bother with the pretence of failed preferential sequencing and would simply leave the ballot blank or spoil the paper in a more overt manner such as scribbles or derogatory comments. The 2004 trial was just as impressive in protecting the electorate's democratic right by eliminating unintentional voting errors (refer table 14)

**Table 14: Voting errors recorded in 2001 and 2004 state general elections<sup>224</sup>**

	2001	2004
Unintentional electronic voting errors	Nil	Nil
Incorrectly sequenced paper ballots	1,141	981
Repeated numbers on paper ballots	1,725	1,315
Total paper voting errors	2,866	2,296

The data obtained over the two electoral events clearly illustrates the high number (5,162) of potentially disenfranchised electors recorded in the ACT. One could assume that should future elections in the ACT be conducted in totality with the use of EVACS, then there is a possibility that such unintentional voting could be eliminated entirely. Such an outcome may be considered positive for democracy and the legitimacy of government.

## Informal voting

A more accurate measure of deliberate ballot spoiling can be obtained by examining the level of informal votes. The number of electronic informal votes was considerably low in 2001, but it is worth mentioning not completely eliminated, at 1.22 per cent compared to 4.27 per cent informal paper ballots. Further analysis of the data reveals that 94 informal electronic votes were caused by electors swiping their barcode to activate the system then pressing the finish key without selecting their preference. This action would cause the EVACS to flash a warning that their vote was informal.

<sup>222</sup> ACT Electoral Commission 2002, p.12

<sup>223</sup> *Ibid.*

<sup>224</sup> ACT Electoral Commission 2002 & 2005.

An additional 109 electors who were issued a barcode did not attempt to use it and either left the polling place with it or simply placed them into a ballot box in the same manner that people place uncompleted paper ballots into ballot boxes. These were recorded as 'discarded votes'.<sup>225</sup>

Although such actions appear to be a deliberate act on behalf of the elector, one element, activating the system but not indicating a preference, could be stopped in the future by amending the software to not permit electors to press the finish key without choosing their preferences. Incidents of individuals who are given a barcode but choose not to use the system will have to be accepted in the same manner as blank paper ballots that are placed into a ballot box.

In contrast the number of informal or discarded paper ballots in 2001 was 7,639 and further analysis reveals that 2,112 were totally blank, 1,556 contained marks, writing and scribbles, and 3,971 contained ticks, crosses and numbers, but not numerically sequential preferences. The Commission stated, although tentatively, that some of the 3,971 informal paper ballots received could be viewed as an indication of intent to vote formally by an elector, and rather than being a protest vote might be a sign of a lack of electoral knowledge. Had these electors used EVACS the number of informal votes might have been reduced.<sup>226</sup> Such assumptions are hard to substantiate but should not be totally dismissed, as is evident from the 2004 trial, and one way to test this hypothesis is to conduct a full scale electronic vote without the option of casting a paper ballot.

The 2004 trial recorded slightly higher levels of both informal and discarded electronic votes, 320 and 209 respectively. Taken together the level of informal and discarded electronic votes was 1.9 per cent in 2004 compared to 1.22 per cent in 2001. The level of informal and discarded paper ballots although still greater than that recorded electronically (2.9 per cent) was less than that recorded in 2001 at 4.27 per cent. The Commission contended that the increasing use of electronic voting could be a contributory factor in the decrease in the number of informal paper ballots, because as stated above, a considerable number of paper ballots although marked incorrectly indicate an intention to vote formally; therefore, as more people opt to cast an electronic ballot the incidences of such errors are eliminated due to the system's automatic preference setting.<sup>227</sup>

---

<sup>225</sup> ACT Electoral Commission 2002, p.13

<sup>226</sup> *Ibid.*

<sup>227</sup> ACT Electoral Commission 2005, pp.15-16.

## Chapter Seven: Concluding Remarks

Elections in the future will be different from those experienced today. Electronic evolution and the tides of change will see to that. Aspects of elections such as candidates, political parties, ballot papers and counting methodologies, be they first past the post or preferential, will remain largely unchanged. The difference will be mainly from the perspective of electors, who will, supported by advances in electronic communication, demand greater convenience and choice in participatory politics.

Although the US electronic voting experience has been less than encouraging, with documented failures of the technology, these failures were neither catastrophic nor fraudulent. Rather, they may be considered more a result of public anxiety and ad-hoc management. The anxiety may stem from the highly publicised failure of older voting systems in 2000, and the torturous counting, recounting and court challenges played out globally in the world's media to find a presidential winner. As a direct result of this legislation was passed to modernise the electoral system and millions of dollars in funds were provided to replace older voting technology.

As one commentator highlighted, “money and technology alone [did] not solve every problem [and]...operator error, negligence and oversight, not equipment failure or mechanical malfunction, cause[d] the vast majority of problems associated with electronic voting”.<sup>228</sup> Nevertheless, the trials will serve to strengthen future endeavours in electronic voting in the US.

Contrast the US experience to that of Estonia, a small country which in comparison is relatively poor and arguably technologically inferior. Yet the Estonians managed to develop and implement an Internet based electronic voting system which incorporated what some commentators believe to be the most robust security measures available in this field. A key difference was the level of preparation and systems testing via mock elections.

Although the participation rate in the Estonian Internet voting trial was low, the system itself worked well with no reported fraud or security breaches. The robustness of the security of the system can be contributed to the incorporation of digital signatures and PKI protocols. Possibly the most important aspect of the Estonian trial was the system testing through mock elections. This allowed the system designers to fine tune the concept, and provided electors with a chance to familiarise themselves with the system, and if necessary update or replace faulty ID cards.

India was an interesting case study in its own right due to the sheer logistics involved. Its experiment resulted in approximately 380 million electors casting a vote on one of the one million plus voting machines in the world's largest experiment in electronic voting to date. India can be considered a quiet achiever in the realm of electronic election modernisation. The approach adopted was to develop a system that was simple to use, understand, and one that was not reliant on sophisticated architecture or software. Although the process was not perfect, it may be considered successful.

---

<sup>228</sup> Mercurio 2003, pp. 238-239.

India developed a system that overcame one of the biggest barriers facing electronic voting; security. This was achieved through simplicity, as the EVM was not reliant on multiple applications or software; it was configured to accomplish the simple task of counting votes and as such, avenues to corrupt the system were reduced.

In the UK an incremental, yet dynamic approach was implemented in their electoral reform agenda. The pilots were conducted over many years, providing invaluable feedback and may be considered dynamic due to their multi-channel voting options. The UK may be perceived as a pioneer in electoral reform due to its innovative approach in offering electors multi-channel voting options, extended voting hours and weekend voting.

The UK conducted pilot schemes in 2000, 2002, 2003 and in each consecutive year the number and variety of electronic channels increased, cumulating in 2003 with 59 local authorities participating in the trials. Of this number 17 offered electronic voting and 14 offered remote electronic voting. In all, 160,000 electors cast an electronic ballot in the May 2003 pilot schemes. Over the course of the trials there were no substantiated incidents of either electoral fraud associated with electronic voting, nor any incidences of 'malicious' or computer virus attacks.

It appears that the general public in the UK are comfortable with new voting structures and technologies, which in all probability is one of the biggest hurdles facing any organisation making a dramatic departure from past practices. This is certainly true for new voting technologies when your clients are citizens and your end product is the formation of executive government.

Australia was also successful in introducing electronic voting. The trial in the ACT which saw the introduction of the EVACS system was effective from many perspectives. There were no substantiated incidents of fraud. Indeed the concerns raised by some opponents of electronic voting, in particular the embedding of malicious software to disrupt or distort election results, was severely hampered, if not totally negated, by the use of 'open source' software. The use of 'open source' software allowed for public scrutiny by computer experts and other concerned individuals.

The use of EVACS was also instrumental in speeding up the counting process and was also an extremely helpful tool for reducing incidents and levels of informal voting. The data from both the 2001 and 2004 trials clearly illustrates the difference in the levels of unintentional voting errors between contemporary paper ballots and electronic ballots.

This paper has shown that the concept of electronic voting is challenging with many competing views for and against the widespread adoption of such technologies. The concerns raised are valid but at the same time not insurmountable. The take-up of electronic voting will not be revolutionary or realised within a short time frame. Change will be incremental and will require an increase in the level of public confidence and familiarity, in much the same way as trust in ATM technology and Internet banking systems was required before widespread adoption.

## Appendices

### Appendix One: Matrix of Voting Technologies by Criterion

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
<b>Accessibility</b> How well the different voting channels perform in relation to voter access, and to what extent, if any, are voters excluded.	<p>Elections in WA are conducted according to the <i>Electoral Act 1907</i>.</p> <p>Accessibility is considered adequate, although voter behaviour is changing.</p> <p>Data from the 2005 State general election reveal a growing trend in early voting prior to the actual polling day.</p> <p>For example, 85,639 early votes were issued in 2005, an increase of 19,385 or 29.26%, compared to 2001.<sup>231</sup></p> <p>There could be a number of reasons for this, from elector awareness such an option exists, to the timing of the</p>	<p>As with voting at a polling place, postal voting is conducted according to the <i>Electoral Act 1907</i>.</p> <p>Postal voting is becoming more popular with electors.</p> <p>Data from the 2005 State general election reveal a growing trend in postal voting.</p> <p>For example, 50,419 or 4% of electors applied for a postal vote, compared to 39,080 in 2001.<sup>232</sup></p> <p>Once again, any premise as to why this</p>	<p>I-voting has the potential to be accessible to a significant number of electors.</p> <p>Data from the ABS indicate that over 60% of the population accessed and used the Internet during 04–05.<sup>234</sup></p> <p>Similar usage trends were recorded in WA from survey data collected immediately after the 2005 State general election.<sup>235</sup></p> <p>Unlike contemporary polling places i-voting is not reliant on</p>	<p>Of all the channels available to facilitate the introduction of new electronic voting methods, the household telephone has the highest penetration rate.</p> <p>Data from the ABS indicate that over 95% of households have a telephone.<sup>236</sup></p> <p>The accessibility merits of this channel are similar to that of i-voting, i.e. the individual can cast a vote at a time of their choosing from the comfort of their own</p>	<p>The potential accessibility of mobile phones to cast a vote is quite high.</p> <p>Data from the ABS indicate that in 2002, over 70% of households had access to a mobile phone.<sup>237</sup></p>	<p>iDTV is a relatively under utilised in Australia.</p> <p>Figures compiled by Digital Broadcasting Australia estimate that at March 2006, 17.9% of Australian homes had access to 'free to view digital television'.<sup>238</sup></p> <p>This platform is predominately used for enhanced viewing and programming and is capable of allowing viewers to participate in live programs and polls.</p> <p>Typically viewers</p>	<p>Direct recording equipment, such as touch screen terminals, are typically owned or leased by the relevant electoral authority.</p> <p>There placement is determined by the relevant electoral authority and they need not be static, so they can be moved from one location to another.</p> <p>In terms of accessibility, DREs offer the same level of convenience, or</p>

<sup>229</sup> Interactive voice recognition (IVR) similar to that used by telephone banking and other commercial telephony services.

<sup>230</sup> Direct recording equipment (DRE) typically a computer terminal screen with touch screen menus, similar to automatic teller machines.

<sup>231</sup> Western Australian Electoral Commission, *2005 Western Australian State General Election, Election Report*, 2006, p.17.

<sup>232</sup> *ibid*, p.18.

<sup>233</sup> Western Australian Electoral Commission, *General information: Local Government Elections Section*, viewed 20 Jun 2006 <<http://www.waec.wa.gov.au/frames.asp?section=local>>.

<sup>234</sup> Australian Bureau of Statistics, *Household use of Information Technology 2004–2005*, ABS cat. no. 8146.0, Canberra, 2005, p.12.

<sup>235</sup> Western Australian Electoral Commission, 2005, *Report on the Western Australian Election Commission Survey of Voters–State General Election 2005*, p.12.

<sup>236</sup> Australian Bureau of Statistics, *Australian Social Trends Housing and Lifestyle: Household amenities*, ABS cat. no. 4102.0, Canberra, 2001.

<sup>237</sup> Australian Bureau of Statistics, *Measures of a knowledge-based economy and society. Characteristic: Household and individual use of ICT*, ABS cat no. 13770.0, Canberra, 2003.

<sup>238</sup> Digital Broadcasting Australia, *Free to view digital television sales top 1.5 million*, 2006.

<sup>239</sup> The Electoral Commission, *Pilot scheme evaluation Kerrier District Council 1 May 2003 Part A*, 2003a, p.19.

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
	<p>election that coincided with a post-Christmas holiday period.</p> <p>Although it remains pure conjecture as to why electors are opting to vote early, as oppose to voting in person, it might be a simple convenience measure.</p> <p>People's lives, work and leisure times have altered drastically over the decades, with people working weekends, nights, and increasingly in remote locations, all of which puts pressure on an individual to carry out their civic duty within the specified time-frame.</p> <p>In this context it could be argued that although this form of voting is sufficient for a vast majority, a significant number of electors find attendance voting either inconvenient or too restrictive for their contemporary lifestyles.</p>	<p>trend is growing is mere conjecture; however, it is probably for the same reasons of convenience discussed in relation to voting at polling places.</p> <p>Alternatively, the use of postal votes in State general elections might be due to their growing use in local government elections, hence making this option more familiar with the electorate.</p> <p>In May 2005, 85% of electors who participated in a local government election cast a postal ballot, making this method the most dominant means by which electors now choose to participate in local decision-making.<sup>233</sup></p>	<p>physical locations, thus negating any access barriers in the built environment.</p> <p>Although the Commission provides 'drive-in' polling places and parking bays for people with limited mobility, on occasion these measures can still be insufficient or demand so great that some people are disadvantaged.</p> <p>I-voting could help alleviate such impediments or inconvenience for people with disabilities, as they could cast a vote from home or place of residence.</p>	<p>residence.</p> <p>The potential for physical barriers to impede access to conventional polling places, even when steps are taken to reduce their prevalence and impact, are mitigated as no actual attendance is required.</p>		<p>engage by using their television remote control to transmit messages or select certain aspects of live programs.</p> <p>Of all the channels available to facilitate electronic voting, iDTV has the least penetration in Australia and accordingly is the least accessible.</p> <p>In one UK trial that offered this channel it was the least popular, with only 228 votes, or 1.3%, compared to the Internet which was used by 1,665, or 9.4% of voters.<sup>239</sup></p>	<p>inconvenience, as attendance voting due to the requirement on electors to attend a polling place in person to cast a vote.</p>
<p><b>Access barriers</b></p> <p>Potential exclusionary barriers or restrictions that</p>	<p>People with physical disabilities or the aged may have difficulty accessing a polling place due to a lack of suitable access ramps or adequate parking near the location.</p>	<p>In some instances postal ballots could be a barrier for the visually impaired if the text is too small to read.</p> <p>Printing and distribution errors may lead to some</p>	<p>The introduction of new technologies inevitably creates a level of apprehension amongst users, particularly if there is a knowledge deficit and</p>	<p>As is the case with all new technologies there is a potential for a knowledge deficit.</p> <p>In relation to telephones this is considered less of an</p>	<p>One conceivable drawback associated with mobile technology is linked to their very design purpose, mobility.</p> <p>Mobile telephones are</p>	<p>Until the digital television market matures in Australia it is unlikely that this option would be viable in the short-term.</p> <p>iDTV as a medium to</p>	<p>Essentially access barriers are the same as those identified in relation to voting at a polling place.</p> <p>There could also be some form of</p>

<sup>240</sup> Western Australian Electoral Commission, 2005 *Western Australian State General Election, Election Report*, 2006, p.18.

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
may hinder or restrict participation.	<p>To lessen such issues the Commission encourages people with limited mobility to register as an 'early voter' and to cast their ballot by post, in addition the Commission offers 'drive-in' voting for electors with disabilities.</p> <p>During the 2005 State general election nine drive-in polling places were offered and 2,989 electors cast a ballot this way.<sup>240</sup></p> <p>This figure represents a 17% reduction on 2001 figures, where 3,591 ballots were cast.</p> <p>Decline in 'drive-in' participation may suggest that this method is not a viable option for electors with mobility constraints.</p>	<p>electors losing their right to vote.</p> <p>During the 2004 federal election, a glitch in the Australian Electoral Commission's (AEC) automated vote issuing system led to a delay in the production and distribution of postal voting material.</p> <p>The AEC contends that this could be a contributory factor as to why 3.9% of postal vote applicants failed to cast a vote, an increase of 63% compared to 2001, and why 568 postal vote certificates were sent to the wrong address.<sup>241</sup></p> <p>Electors in remote areas may have restricted postal services, limited to weekly or twice weekly, due to distances from regional centres and limited users of the service, i.e. remote cattle stations or indigenous communities.</p>	<p>unfamiliarity about how the system works.</p> <p>Consideration must be given to the 40% of electors who have no access to the Internet.</p> <p>Although theoretically these electors could use public access points such as libraries, one could assume that for this group any knowledge deficit would be greatest.</p> <p>The UK Electoral Commission noted in its evaluation report, that no single electronic voting channel would be totally accessible to all electors; however, contends that multiple channels increases accessibility by providing greater choice.<sup>242</sup></p> <p>The Commission concurs with this view and intends to continue to offer multiple voting channels to electors.</p>	<p>issue in Australia.</p> <p>It would be reasonable to assume that a majority of Australians are comfortable with this method, and have used this kind of service to access information or pay bills.</p> <p>However, unlike voting at a traditional polling place, where ballot papers and candidate information is presented to an elector upon arrival, telephone voting requires all this information to be sent to the elector.</p> <p>This raises the question of additional costs for the relevant electoral commission and also issues regarding multilingual support, i.e. what language should be used and will the receiver be able to read it.</p>	<p>designed for communicating on the move, and as such, reception and background noise could be a significant barrier to participation, particularly if the user has a hearing impairment.</p> <p>Additionally, mobiles can be affected by 'black spots' where communication is not possible due to limited signals and reception.</p> <p>Also this channel requires information to be posted to the elector, which raises the same issues as discussed in relation to touch-tone telephony.</p>	<p>facilitate an election would impose significant costs on the elector as they would be required to purchase a new television.</p> <p>Nor is this channel without limitations or impediments.</p> <p>A disability 'access audit' conducted in 2003, as part of the Kerrier district e-voting pilot evaluation, noted that although the use of text on plain backgrounds was a positive aspect of this medium, there were concerns that the remote controls may prove difficult for people with visual or mobility impairments.<sup>243</sup></p>	<p>apprehension on the part of some electors who are unfamiliar or unsure about using such technologies.</p> <p>Although as they work in a similar fashion as an ATM this might not be such an issue, and election officials would be on hand to assist.</p>

<sup>241</sup> Australian Electoral Commission, *Results released from inquiry into postal voting at 2004 election*, media release, 2004.

<sup>242</sup> The Electoral Commission, *The shape of elections to come a strategic evaluation of the 2003 electoral pilot schemes*, 2003b, p. 69.

<sup>243</sup> The Electoral Commission, *Pilot scheme evaluation Kerrier District Council 1 May 2003 Part A*, 2003a, p.20.

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
<p><b>Multilingual Support</b></p> <p>How well the different channels perform in relation to elector support and accommodation of different languages.</p>	<p>The Commonwealth translating and interpreting service identified 22 languages requiring translation in WA.</p> <p>The Commission offers multilingual support to this identified group through three avenues; an how-to-vote guide, the Internet, and a telephone translation service.</p> <p>The how-to-vote guide was compiled and made available in the 22 languages, and was accessible at every early voting (in person) office, polling places and on the Commissions web site.</p> <p>In addition information was made available on the Commission's web site in conjunction with a telephone interpreting service which was available for any queries.<sup>244</sup></p>	<p>In State general elections support is the same as that offered at polling places.</p> <p>Local government elections are different, as typically all electors in the respective council wards are automatically sent candidate information and election packages.</p> <p>Unless prior arrangements are made the election package would be in English.</p> <p>Although assistance could be provided upon request, there is the possibility that whole package might be discarded due to a language barrier.</p>	<p>An advantage of computer technology is that it can incorporate a great deal of information and support services and be readily accessible to multiple people from various locations simultaneously.</p> <p>The Internet provides the opportunity to expand and enhance current multilingual support at a fraction of the cost.</p> <p>Any language could be incorporated into the system and made available 24 x 7.</p> <p>Additional services can be identified and added to the system on an 'as needs basis', making the whole service more dynamic.</p>	<p>Multilingual support can be easily adopted and managed in much the same manner as that utilised in i-voting.</p> <p>Electors could key in the relevant number and receive an automated message in any number of languages; once again this system becomes more dynamic and can be updated as required.</p>	<p>Mobiles could conceivably provide similar multilingual support as land-lines.</p>	<p>iDTV could conceivably provide similar multilingual support as that offered by i-voting.</p>	<p>DRE can be configured in numerous ways and preloaded with a multitude of different languages; in essence they can incorporate all the same convenience measures as i-voting, with the exception being that the elector has to go the poll, rather than the polls coming to the elector.</p>
<p><b>Visual and audio support</b></p> <p>The measure of assistance offered, if any, to electors with</p>	<p>During the last State general election in 2005, the Commission took a number of steps to assist those electors who were afflicted with a visual impairment.</p>	<p>The very nature of postal voting places limitations on complimentary services, due to cost and lack of knowledge of who needs</p>	<p>Electronic ballots can be enlarged to a size that is suitable to the individual, and can be further enhanced through audio</p>	<p>Telephones have evolved to such an extent that they now offer a wide range of features to assist people with hearing impairment and, can</p>	<p>Mobiles could conceivably provide similar support as land-lines, but as mentioned earlier, reception and background noise would probably reduce</p>	<p>iDTV could conceivably provide a similar level of audio and visual support as that offered by i-voting.</p> <p>As previously</p>	<p>In the same way that DREs can be preconfigured to assist in the provision of multilingual support, they can also be</p>

<sup>244</sup> Western Australian Electoral Commission, 2005 *Western Australian State General Election, Election Report*, 2006, p.11.

<sup>245</sup> *ibid.*

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
visual and hearing impairment.	<p>This included the provision of eleven 'video magnifiers' made available at some early voting (in person) locations and polling places throughout the state to assist the visually impaired.</p> <p>In addition, magnifying sheets capable of increasing the print on ballot papers were available at all 'early voting' locations.</p> <p>The locations were advertised in <i>The West Australian</i> on polling day, the Commission's web site, and published in <i>Election News</i> a publication produced by the Commission.<sup>245</sup></p>	<p>what.</p> <p>Consequently, assistance and support is limited, and if an elector has to physically attend a location to obtain assistance in completing a ballot, e.g. to use a magnifier, it negates any convenience gained in the first place.</p>	<p>assistance.</p> <p>In addition, audio could not only help the elector to cast a vote, it could also be used by candidates to convey a verbal message that might not be accessed through traditional formats such as print.</p> <p>Like the provision of multilingual support, visual and audio assistance could be incorporated into the system and made available 24 x 7.</p>	<p>be reasonably assumed capable of assisting an elector to cast a vote.</p> <p>Deafness Resources Australia has further information regarding services to assist people with hearing impairment.<sup>246</sup></p> <p>Telephones do not incorporate audio visual technology, and as such this channel offers little in the way of assistance for the visually impaired.</p>	<p>the benefits of audio enhancement.</p>	<p>mentioned, a disability access audit conducted in the UK indicated that iDTV was ideally suited to conveying text on a screen.</p>	<p>preloaded with visual and audio assistance tools for the visually or hearing impaired.</p> <p>Text and ballot papers can be produced in bigger scales, and audio prompts could be delivered either through speakers or headphones as a cursor crosses over sections of the screen.</p>
<p><b>Secrecy</b></p> <p>To what extent, if any, the different voting channels facilitate the casting of a ballot in secret.</p>	<p>In Australia, the concept of the 'secret' ballot is a fundamental part of the democratic process.</p> <p>Electors are able to vote for a candidate or political party of their choice free of interference or coercion, and once a choice has been made no other individual is aware of how they voted.</p> <p>It is not inconceivable to suggest that voting at a public polling place is the most effective way of managing</p>	<p>The act of casting a ballot from another location other than a managed polling place does not reduce ones entitlement to a secret ballot.</p> <p>However, it does introduce an element of risk that coercion could be applied.<sup>247</sup></p> <p>The nature of postal voting means that the act of completing a ballot is conducted away</p>	<p>I-voting should not represent any greater threat of coercion to an elector from that which already hypothetically exists in relation to postal voting.</p> <p>The act of electronic voting, just like the act of postal voting, is conducted away from the direct supervision of election officials so the risk level by extension must be the</p>	<p>The notion of coercion could be an issue in the same sense as postal voting.</p> <p>For voters with disabilities or literacy constraints, the use of touch-tone telephones could provide an alternative method of voting which negates the need for third party involvement.</p> <p>However, whilst this method provides an</p>	<p>The notion of coercion could be an issue in the same sense as postal voting.</p> <p>The strengths and weakness are the same as touch-tone telephony.</p> <p>However, unlike land-lines, predominately located within the confines of a private household, mobiles can be used anywhere which could</p>	<p>The notion of coercion could be an issue in the same sense as postal voting.</p> <p>However, given that the family television is usually centrally located within the household, finding an opportune time to cast a 'secret' ballot maybe problematic.</p>	<p>Same level as voting at polling places as people will still be required to attend in person.</p> <p>For voters with disabilities, visual impairment or literacy constraints, DREs could provide an alternative method of voting which negates the need for third party involvement.</p>

<sup>246</sup> <http://www.deafnessresources.net.au/>

<sup>247</sup> Barry et al. 2002, p.16.

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
	<p>and limiting all forms of coercion and interference.</p> <p>Due to the whole process being managed by election officials, who observe and restrict interference by other individuals.</p> <p>However, secrecy of ones vote might be compromised for people with disabilities, visual impairment or literacy constraints, if they require assistance in accessing a voting screen or to cast a vote.</p>	<p>from the watchful eye of election officials.</p> <p>For that reason it has been suggested that individuals casting a postal ballot could hypothetically face undue influence to vote for a candidate against their wishes.</p> <p>However, as increasing numbers of electors are opting to cast a postal ballot in State general elections, and increasingly local government elections are decided via postal ballots, it appears electors have accepted this level of risk without any reported incidents of coercion.</p> <p>As is the case with voting at polling places, people with disabilities, visual impairment, or literacy constraints, may require assistance and as such may lose the notion of a secret ballot.</p>	<p>same.</p> <p>For electors with disabilities, visual impairment or literacy constraints, the Internet could provide an alternative method of voting which negates the need for third party involvement.</p> <p>Conceivably, i-voting could allow such electors who have historically relied on another for assistance to cast a vote, to listen to an audio transmission or follow large visual prompts on a screen.</p> <p>Thus in this scenario the elector can, and maybe for the first time, cast unassisted ballot and realise the notion of the 'secret ballot'.</p>	<p>audio assistance measure, it cannot provide visual assistance.</p> <p>Given that this method requires written voting and candidacy information to be sent to electors, the notion of the 'secret' ballot might be compromised.</p>	<p>diminish ones perception of privacy.</p> <p>Consequently the public nature of mobiles may be a barrier to participation for some.</p>		
<p><b>Accuracy</b></p> <p>To what extent, if any, the different voting channels facilitate the accurate casting</p>	<p>The tradition of manually checking and counting ballots can be considered sufficient and accurate.</p> <p>Technology plays a role in the process and it is now common</p>	<p>The process of counting postal ballots is the same as those used to count ballots at a polling place, thus the strengths and weaknesses are the</p>	<p>It is widely accepted that computers can perform calculations fast and accurately.</p> <p>The use of a computer to cast a ballot appears</p>	<p>Accuracy and benefits considered the same as those associated with i-voting.</p>	<p>Accuracy and benefits considered the same as those associated with i-voting.</p>	<p>Accuracy and benefits considered the same as those associated with i-voting.</p>	<p>Accuracy and benefits considered the same as those associated with i-voting.</p>

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
and counting of ballots.	<p>practice for electoral authorities to use computers 'to conduct complex proportional representation [counts], such as the Senate count, by entering the handwritten preferences into computer systems'.<sup>248</sup></p> <p>This process is not infallible as recounts have revealed.</p> <p>This was the case in 1998, where a close result in the Australian Capital Territory (ACT) electorate of Molonglo necessitated a recount which revealed the original count was in error.<sup>249</sup></p> <p>There is also a requirement on the voter to be accurate in the way they mark their ballot.</p> <p>Incorrectly marked ballots are termed 'informal' and are not taken into consideration in deciding who should govern, and votes cast in this manner disenfranchises the elector.</p> <p>During the 2005 State general election, informal votes were recorded at the districts of Bunbury, Belmont and Dawesville, of 4.83%, 5.51% and 4.72% respectively.<sup>250</sup></p> <p>The current manual process of casting and counting of ballots</p>	same.	<p>to be a logical next step in further enhancing an already automated process, reducing the double handling of ballot papers, and thus eliminating the human error factor associated with re-keying elector intentions.</p> <p>Additionally, the use of paper ballots cannot resolve the issue of accidental or 'informal' voting, whereby an elector mistakenly (or deliberately) marks the ballot paper incorrectly.</p> <p>I-voting can eliminate incidents of 'informal' voting, as the system can be programmed to not accept informal votes.</p> <p>Alternatively, 'informal votes' could be accepted and recorded as a legitimate protest vote, if after sufficient warning an elector chooses to proceed and cast an 'informal vote'.</p>				

<sup>248</sup> Green 2000, p.1.

<sup>249</sup> Elections ACT 2002, p20.

<sup>250</sup> Western Australian Electoral Commission. *Elections WA State General Election Results*, viewed 28 June 2006 <[http://www.electionswa.com.au/la\\_districts.htm](http://www.electionswa.com.au/la_districts.htm)>.

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
	can not reduce incidents of informal voting.						
<p><b>Deliberation</b></p> <p>To what extent, if any, the different voting methods facilitate deliberation.</p>	<p>From the perspective of the Commission deliberation is not part of the electoral management process; however, dissemination and content of candidate information does come under its remit</p> <p>In the context of polling day there is little or no deliberation; political party activists, candidates and other interested individuals are restricted from entering polling places to canvass votes.</p> <p>On polling day the nearest incidence or resemblance of deliberation is the act of handing out 'how-to-vote cards' from a predetermined distance outside the actual polling place by political party activists.</p> <p>All other forms of deliberation, or political discussion, are of a nature that would be accessible to electors' without consideration of the voting method.</p>	<p>Postal voting in State general elections has the same level of deliberation as that found in attendance however, the only difference being the lack of contact with political party representatives distributing how to vote cards on election day.</p> <p>In the case of local government elections, which are increasingly conducted via postal ballots, candidate profiles are automatically sent direct to all eligible electors</p> <p>Typically the information includes the candidate's biography and particular viewpoints on local issues, and is sent in advance of the election day, thus giving electors' time to evaluate their options and to ask questions of the candidates.</p> <p>However, the act of casting an early postal ballot, either in local government or state general elections, may well result in electors being denied the</p>	<p>From the perspective of the Commission, the adoption of the Internet or any other form of electronic voting, the only difference being the lack of contact with political party representatives distributing how to vote cards on election day.</p> <p>From the perspective of the Commission, the adoption of the Internet or any other form of electronic voting, the only difference being the lack of contact with political party representatives distributing how to vote cards on election day.</p>				

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (IDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
		opportunity to take into consideration last minute developments.					
<b>Security</b> To what extent, if any, the different voting channels are secure from malicious attack.	<p>Australia is a stable democracy and contemporary methods of casting a ballot are considered reasonably secure.</p> <p>At polling places secure ballot boxes are used for receiving marked ballot papers, utilising numbered plastic security ties to prevent unlawful tampering.</p> <p>At the end of the election period the ballot boxes are transported to the designated counting location for election officials to count under the watchful eye of election scrutineers.</p> <p>An individual could hypothetically spoil ballot papers by the simple act of pouring liquid into the ballot box.</p> <p>Alternatively, a committed individual(s) could intercept the ballot papers during transportation to the counting location.</p> <p>Such an act, however unlikely, could lead to the disenfranchising of thousands of individuals, and with no backup system voter</p>	<p>The security of postal ballots is out of the control of election officials until they are received at the official counting location, and to date this method of voting is considered secure, even with the lack of official control over the voting process.</p> <p>Essentially there are few security measures in place prior to the receipt of the postal vote, and hypothetically ballot papers can be lost, stolen, or delayed in the post.</p> <p>Once again in the realm of supposition, ballot papers can be deliberately destroyed during transportation or stolen from the elector's mail box in an act of malicious fraud or election disruption.</p>	<p>The adoption of new technologies to facilitate elections includes an element of risk that needs to be taken into consideration as part of a risk management strategy.</p> <p>Risks noted by some commentators involve potential technical limitations of the software to produce a secure environment with adequate safeguards against malicious attack.<sup>251</sup></p> <p>Security issues unique to e-voting include</p> <ul style="list-style-type: none"> <li>- viruses,</li> <li>- hacking into computer systems, (corrupting data)</li> <li>- system flooding, (incapable of coping with demand)</li> <li>- and power</li> </ul>	<p>Considered to have the same strengths and weaknesses as i-voting.</p>	<p>Considered to have the same strengths and weaknesses as i-voting.</p>	<p>Considered to have the same strengths and weaknesses as i-voting.</p>	<p>Typically DREs are used as an 'offline' system, so virus attacks and hacking in the conventional sense is not considered an issue, i.e. hacking into the system through an online and open communication channel.</p> <p>However, it is theoretically possible for malicious attacks to occur through embedded disruptive software being placed into the systems by corrupt officials and software engineers.</p> <p>Alternatively, 'acts of God' and service failure may result in some electors being unable to vote using this system, but as these systems are located at polling places a simple reversion to paper ballots might be possible.</p>

<sup>251</sup> Barry et al. 2002, p.16.

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
	<p>intentions would not be known.</p> <p>In the event of such an act the Court of Disputed Returns would determine whether or not to rerun the election on a district, region or state level.</p>		<p>failure.</p> <p>Strategies could include, amongst others, the use of cryptography and digital signatures to protect data during transmission.</p> <p>Extended voting periods over a few days to negate problems associated with flooding, allowing voters more time and preventing last minute or early morning surges in voting.</p> <p>Hacking will be prevented by incorporating electronic safeguards similar to those used in banks and online bill payment systems.</p>				
<p><b>Authentication</b></p> <p>To what extent, if any, the different voting channels provide elector authentication and identification integrity.</p>	<p>Elector authentication at a polling place could be considered informal.</p> <p>An individual attends a polling place and states a name, declares that they have not already cast a vote at another location and are given ballot papers for the purpose of casting a vote.</p> <p>There is no requirement to produce any identification.</p> <p>Consequently the potential</p>	<p>Elector authentication in postal voting could also be viewed as informal.</p> <p>In local government postal elections all eligible electors on the electoral roll in the district or ward where an election is taking place are sent ballot papers.</p> <p>There is a risk in postal elections that ballot papers may be stolen from letter boxes and</p>	<p>Elector authentication in an electronic environment takes on a completely new dimension, yet a surprisingly familiar one to most Australians who ever used an ATM, paid a bill over the Internet or used Bpay.</p> <p>Typically more robust and high-tech; utilising a combination of a voter identification</p>	<p>Elector authentication systems and sequences are similar across the whole range of electronic voting methods discussed in this paper.</p>	<p>Elector authentication systems and sequences are similar across the whole range of electronic voting methods discussed in this paper.</p>	<p>Elector authentication systems and sequences are similar across the whole range of electronic voting methods discussed in this paper.</p>	<p>The process would be identical to that which exists in contemporary attendance voting at a polling place.</p> <p>Electors would make the same declaration, be marked off the electoral roll and shown to a voting screen to vote using a touch screen computer terminal or similar device.</p>

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
	<p>for fraud or 'personation' exists under these circumstances, though there is little evidence to suggest such acts of fraud are common place in Australia.</p> <p>There are procedures in place to detect multiple voting after the event and such checks are routinely carried out by electoral authorities.</p>	<p>fraudulently completed and returned.</p> <p>Unsurprisingly there have been recent instances in both the United Kingdom and Western Australia where this has occurred.</p> <p>However, there are processes in place to detect such fraudulent behaviour, such as checking the signature on the ballot returns against the original signature of the elector which minimise risk and detect fraud.</p>	<p>numbers (VIN) supplied by the Electoral Commission linked to the electoral roll, and a personal identification number (PIN) creating a two point verification sequence. This can be supported by a third identification level such as the date of birth of the elector.</p> <p>In addition, the contemporary method of relying on the honesty of individuals to only vote once at one location could become a matter of the past, as electronic voting detects and disallows such behaviour in 'real time' by removing the VIN from the system once a valid vote has been cast.</p> <p>As a result of these electronic authentication measures it could be argued that electronic voting brings a new level of robustness and security to an informal system.</p>				
<b>Timeliness</b>	In the age of 'instant news' election officials are	Same strengths and weaknesses as	I-voting, and by extension electronic	Can be assumed that ballot counting would			

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
To what extent, if any, the different voting channels facilitate the timely counting of ballots.	<p>constantly pressed to update and confirm results quickly to enable media outlets to provide commentary to their audiences.</p> <p>Whilst in most cases election trends for specific seats are usually known within the first few hours of the poll closing, the actual result of the election can take a good deal longer.</p> <p>In some instances the election results can take days in close marginal seats.</p> <p>The current method of manual counting is slower than it would be using internet voting and labour intensive, and as discussed earlier it is not infallible with occasional errors occurring leading to recounts.</p> <p>Delays to processing are also incurred in the more complex areas of processing declaration votes, and LC ballots.</p>	attendance voting.	<p>counting, would greatly enhance and speed up the present process.</p> <p>Currently, postal and absent votes can not be included in election night tallies until the identification of the elector has been substantiated.<sup>252</sup></p> <p>Given that there are a growing number of electors who, for whatever reason, opt to cast a postal vote. The introduction of i-voting as alternative to postal voting would significantly enhance the timeliness of election night results.</p> <p>I-voting would allow for these votes to be counted and included immediately as the identification process has already been established at the beginning of the process.</p>	be conducted more efficiently and effectively, whilst removing the prospect of human error.	be conducted more efficiently and effectively, whilst removing the prospect of human error.	be conducted more efficiently and effectively, whilst removing the prospect of human error.	be conducted more efficiently and effectively, whilst removing the prospect of human error.
<b>Verifiability</b> To what extent, if any, the different voting channels allow for verification	Currently, verification of election results are managed and overseen by election scrutineers, political party officials and other interested parties who attend the counting	Verification of postal votes is conducted in the same manner as that described for attendance voting at a polling place and consequently is	Verification is not possible in the traditional sense, in particular from the perspective of election scrutineers who can	Verification methodology would be similar across the whole range of electronic voting methods discussed in	Verification methodology would be similar across the whole range of electronic voting methods discussed in	Verification methodology would be similar across the whole range of electronic voting methods discussed in	Verification methodology would be similar across the whole range of electronic voting methods discussed in

<sup>252</sup> Barry et al. 2002, p.17.

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
of election results..	<p>location and visually observe the count.</p> <p>This method of physical observation consumes a considerable amount of time and carries on late into the night.</p> <p>Nevertheless, the critical advantage of the paper ballot is it allows for verifiability of the election result.</p> <p>This verifiability is possible due to the audit trail produced by paper ballots, and in the case of close contests or disputed returns, the ballots may be recounted.</p> <p>Typically, interested observers and election officials check each ballot paper to ensure the elector's intention gets contributed to the respective candidate.</p> <p>In doing so, they ensure that informal votes are excluded from the process and ballot papers which are ambiguous, due to unclear marking or preferences, are quarantined and adjudicated on accordingly.</p> <p>Although this method has been used, and has sufficed for many years, it is not perfect and it could be</p>	<p>prone to the same benefits and limitations.</p>	<p>no longer visually observe the process.</p> <p>This may cause disquiet amongst some circles, but overtime should become less of an issue as people adapt to the changes and use new methodologies for scrutineering purposes.</p> <p>One avenue for electronic scrutineering could evolve through the use of open source code software, whereby access is provided to the software program for verification purposes.<sup>253</sup></p> <p>Electronic scrutineers would function in the same manner as their traditional counterparts, by ensuring the system is fair and that the program is capable of doing what it is designed to do, that is, receive, verify and allocate votes to the</p>	<p>this paper.</p>	<p>this paper.</p>	<p>this paper.</p>	<p>this paper.</p> <p>However, as people still have to attend a polling place to cast a ballot, provision could be made for the printing, storing and counting of paper receipts.</p> <p>The production of receipts from DRE would not only be time consuming and expensive, it would also defeat the purpose and efficiency gains associated with electronic voting.</p>

<sup>253</sup> This approach is advocated by Barry et al. (2002, p.17), who assert that 'electoral commissions should be required to have any source code certified by an appropriate authority [and additionally] open to any candidate, scrutineer or registered political party for their own verification'.

Criterion	Voting at a Polling Place	Postal Voting	Internet (i-voting)	Touch-Tone Telephony (IVR) <sup>229</sup>	SMS Text	Interactive Digital Television (iDTV)	Touch Screen Terminals (DRE) <sup>230</sup>
	<p>considered inefficient and flawed given that recounts, and by extension reverification, have revealed errors.</p>		<p>respective candidate.</p> <p>The ACT conducted an electronic voting trial in 2001, and adopted the approach of utilising 'open source code software'.</p> <p>This allowed interested parties or individuals to scrutinise the software and to verify whether or not it could function as intended.</p> <p>Alternatively, verification standards can be developed to test and certify system software for compliance. The testing can be undertaken by independent bodies following mandated guidelines.</p>				

**Appendix Two: Salford pilot scheme debriefing session, 11 May 2000<sup>254</sup>**

Reported problems	Suggested general improvements
Insufficient setup time had been allowed at the polling place, resulting in the poll being opened at 8.05a.m.	Increase the number of technical support staff to cater for machine breakdown. It is acknowledged that TIS have recognised this situation and have since taken steps to train more of their own staff to improve support for future occasions.
Confusion over the legality of one laptop and its rejection by a presiding officer, led to a 30 minute delay in opening the poll. Electors who insisted upon voting during this time were issued with tendered ballot papers which were classed as normal votes and included in the count.	Employ two poll clerks instead of one. This would allow one clerk to assist electors in the use of the machine when recording their votes while maintaining normal staffing levels to deal with electors.
Voting machine breakdowns were reported regularly over the day. At one polling place there were an estimated twenty breakdowns.	Provide two laptops to increase rate of elector processing.
Technical back-up response to requests to TIS and GES for assistance was slower than anticipated. In one instance an hour elapsed before a response was made to a request for assistance.	Use hand held card readers which would have immediate response in processing elector information, instead of 30 seconds experienced at this election.
Card readers took 30 seconds to process elector information and later in the day as more people turned out to vote lengthy queues developed.	Provide bar codes on poll cards for processing elector information.
The close proximity of the machines in one polling place resulted in electors inserting their cards into the wrong machine causing them to fail.	Instructions to electors should be included on all screens, not just the first one, and be expressed in plainer English.
Electors complained that because screens were angled towards them electors in adjacent booths could see their choice of candidate.	Machine screens should be positioned at a lower level to improve security.
Many electors requested assistance from polling staff when casting their vote. Poll clerks usually provided assistance but at busy periods this left the presiding officer isolated in dealing with issuing cards to other electors in the queue.	A facility to return to previous screens, particularly screen showing candidates details, should be incorporated into the system.
Some electors had difficulty inserting their card into the machine, particularly the elderly and arthritic.	Number of electronic voting machines at each polling station needs to be increased to three instead of two.
Instructions on how to use the machines were only shown on the first of three screens. Some electors forgot the relevant instructions as they progressed through the voting process.	Where two polling stations are sited at one polling place segregation of machines needed to be improved to prevent electors putting cards into wrong machines.
One elector managed to put their card at the back of the screen causing machine failure.	At training sessions the operation of laptop computers should be demonstrated.

<sup>254</sup>

*ibid.*

## Bibliography

ACT Electoral Commission. (2002). *The 2001 ACT Legislative Assembly Election Electronic voting and counting system Review*. Australian Capital Territory, Canberra.

ACT Electoral Commission. (2005). *Electronic voting and counting system review: The 2004 ACT Legislative Assembly Election*. Australian Capital Territory, Canberra.

Australian Bureau of Statistics. (2005). *Household Use of Information Technology* (8146.0). Canberra: Online, viewed 10 May 2006  
<[http://www.ausstats.abs.gov.au/Ausstats/subscriber.nsf/0/CA78A4186873588CCA2570D8001B8C56/\\$File/81460\\_2004-05.pdf](http://www.ausstats.abs.gov.au/Ausstats/subscriber.nsf/0/CA78A4186873588CCA2570D8001B8C56/$File/81460_2004-05.pdf)>.

Australian Institute of Criminology. (2002). *Electronic Voting: Benefits and Risks* (1-6, No 224). Canberra: Commonwealth Government.

Beary, H. (2004). *Gearing up for India's electronic election*. BBC News Online. Viewed 03 July 2006  
<[http://news.bbc.co.uk/1/hi/world/south\\_asia/3493474.stm](http://news.bbc.co.uk/1/hi/world/south_asia/3493474.stm)>.

Californian Secretary of State. (2003). *Secretary of state's ad hoc touch screen task force report*. California, USA. Viewed 04 July 2006  
<[http://www.ss.ca.gov/elections/taskforce\\_report\\_entire.pdf](http://www.ss.ca.gov/elections/taskforce_report_entire.pdf)>.

City of Salford. (2000). *Electronic voting and counting scheme 4<sup>th</sup> May 2000 evaluation report*. Viewed 28 August 2006  
<[http://72.14.203.104/search?q=cache:pqDf7pXW1\\_wJ:www.odpm.gov.uk/stellent/groups/odpm\\_locgov/documents/page/odpm\\_locgov\\_605298.pdf+Salford+\\*Electronic+Voting\\*&hl=en&gl=au&ct=clnk&cd=6](http://72.14.203.104/search?q=cache:pqDf7pXW1_wJ:www.odpm.gov.uk/stellent/groups/odpm_locgov/documents/page/odpm_locgov_605298.pdf+Salford+*Electronic+Voting*&hl=en&gl=au&ct=clnk&cd=6)>.

Congressional Research Service. (2003). *Election reform and electronic voting systems (DREs): Analysis of security issues*. Viewed 04 July 2006  
<<http://www.epic.org/privacy/voting/crsreport.pdf>>.

Diebold Election Systems. (2003). *Checks and balances in elections equipment and procedures prevent alleged fraud scenarios*. North Canton, Ohio USA. Viewed 06 July 2006  
<<http://www2.diebold.com/checksandbalances.pdf>>.

Election India. (2004). *Election News Feb–June 2004*. Election Commission of India. Viewed 25 August 2006  
<[http://www.eci.gov.in/Library&Publications/Lib&Publications\\_fs.htm](http://www.eci.gov.in/Library&Publications/Lib&Publications_fs.htm)>

Elliot, M. (n.d.). *Examining Internet voting in Washington*, viewed 29 July 2004  
<<http://www.electioncenter.org/voting/InetVotingWhitePaper.html>>.

Estonian National Electoral Committee. (2005a). *Statistics of e-voting Municipal elections 2005*. Estonia. Viewed 30 May 2006  
<<http://www.vvk.ee/english/results.pdf>>.

Estonian National Electoral Committee. (2005b). *Internet voting at the Elections of Local Government Councils on October 2005 Report*. Estonia. Report prepared by Ulle Madise, Priit Vinkel, & Epp Maaten. Viewed 30 May 2006  
<<http://www.vvk.ee/english/report2006.pdf>>.

Estonian National Electoral Committee. (2005c). *The National Election Committee E-voting system overview*. Tallinn, Estonia. Viewed 03 July 2006  
<<http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf>>.

European Commission. (2005). *EE: About 1% of votes cast online in Estonian local elections, eGovernment news–19 October 2005–Estonia–eDemocracy*. IDABC. Viewed 03 July 2006  
<<http://ec.europa.eu/idabc/en/document/4999>>.

Fair Election International. (2004a). *Election readiness, it is never too late for transparency: pre-election observation report*. San Francisco, USA. Viewed 03 July 2006  
<[http://www.fairelection.us/observers\\_report1.pdf](http://www.fairelection.us/observers_report1.pdf)>.

- Fair Election International. (2004b). *2004 US Election: An international perspective November 2004 United States observation report*. San Francisco, USA. Viewed 03 July 2006 <<http://www.fairelection.us/fairelectionreport.pdf>>.
- Galston, W (1999). Does the Internet Strengthen Community? Report from the Institute for Philosophy and Public policy, School of Public Affairs, 19 (Fall 1999), 1-8.
- Gibson, Rachel. "Elections online: assessing Internet voting in light of the Arizona Democratic primary. (Abstract)." *Political Science Quarterly* 116.4 (Winter 2001): 561 (24). Expanded Academic ASAP. Thomson Gale. Murdoch University Library. Viewed 04 May 2006 <<http://0-find.galegroup.com.prospero.murdoch.edu.au>>.
- Green, P. (2000). Politics of the Future the Internet and the Electoral Process: Proceedings of the Australian Political Science Association seminar, 5 October 2000, Australian National University. Canberra.
- Internet Policy Institute. (2001). *Report of the national workshop on Internet voting: issues and research agenda*. Viewed 04 July 2006 <<http://fl1.findlaw.com/news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf>>.
- Jones, C. A. (2006) Out of Guatemala?: Election law reform in Florida and the legacy of *Bush v. Gore* in the 2004 Presidential Election. *Election Law Journal*, volume 5, issue 2, pp.121-143.
- Kitcat, J. (2005). *Estonia e-votes*, viewed 03 July. 2006 <[http://www.j-dom.org/h/f/JDOM/blog//1//?be\\_id=244](http://www.j-dom.org/h/f/JDOM/blog//1//?be_id=244)>.
- Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2003). *Analysis of an electronic voting system*. John Hopkins University Information Security Institute technical report (TR-2003-19, July 23, 2003) viewed 04 July 2006 <<http://avirubin.com/vote.pdf>>.
- Kripalani, M. (2004). 'A voting revolution in India? India's new electronic system—built on \$200 machines—could curb fraud and build faith in the process'. *BusinessWeek* Viewed 03 July 2006 <[http://www.businessweek.com/print/magazine/content/04\\_16/b3879074.htm?chan=mz](http://www.businessweek.com/print/magazine/content/04_16/b3879074.htm?chan=mz)>.
- Local Government Association. (2000). *Elections—the 21<sup>st</sup> century model—an evaluation of May 2000 local electoral pilots*. Research Report 14. Viewed 28 August 2006 <<http://www.lga.gov.uk/lga/blg/pb.pdf>>.
- Local Government Association. (2002). *The implementation of electronic voting in the UK research summary*. Viewed 8 May 2006 <[http://www.lga.gov.uk/Documents/Briefing/Our\\_Work/BLG/Infoage/LGASummary.pdf](http://www.lga.gov.uk/Documents/Briefing/Our_Work/BLG/Infoage/LGASummary.pdf)>.
- Mercurio, B. (2003). 'Beyond the paper ballot: Exploring computerised voting'. In G. Orr., B. Mercurio., & G. Williams (Eds.), *Realising Democracy: Electoral Law in Australia* (pp. 230-242). Sydney: Federation Press.
- Reich, Eugenie Samuel, and Celeste Biever. "The great American voting experiment: e-voting is supposed to be more accurate, but what if votes can just as easily go missing or be miscounted? (This week: electronic voting)." *New Scientist* 184.2469 (Oct 16, 2004): 6(3). Expanded Academic ASAP. Thomson Gale. Murdoch University Library. 01 May 2006 <<http://0find.galegroup.com.prospero.murdoch.edu.au>>.
- Rohde, D. (2004). 'On new voting machine, the same old fraud'. *The New York Times*. Viewed 24 August 2006 <<http://select.nytimes.com/gst/abstract.html?res=FB0F11F93A5E0C748EDDAD0894DC404482>>.
- Rubin, A. D. (2002). *Security considerations for remote electronic voting over the Internet*, viewed 06 July. 2006 <<http://avirubin.com/e-voting.security.pdf>>.

- Santosus, M. (2004). The lowdown on e-voting. *CIO Online*. Viewed 07 April 2006 <<http://www.cio.com.au/pp.php?id=558873322&fp=4&fpid=21>>.
- Sheeter, L. (2005). 'Estonia forges ahead with e-vote'. *BBC News online*, 14 October. Viewed 03 July 2006 <<http://news.bbc.co.uk/2/hi/europe/4343374.stm>>.
- Srinivasan, S. (2004). 'E-voting in India can't remove possibility of fraud'. *USA Today*. Viewed 03 July 2006 <[http://www.usatoday.com/tech/world/2004-05-12-india-evote\\_x.htm](http://www.usatoday.com/tech/world/2004-05-12-india-evote_x.htm)>.
- State of Maryland General Assembly. (2004). *Trusted agent report Diebold AccuVote-TS voting system*. Department of Legislative Services, Maryland. Viewed 06 July 2006 <[http://www.raba.com/press/TA\\_Report\\_AccuVote.pdf](http://www.raba.com/press/TA_Report_AccuVote.pdf)>.
- The Electoral Commission. (2002a). *Modernising elections: a strategic evaluation of the 2002 electoral pilot schemes*. UK Government. Viewed 8 May 2006 <<http://www.electoralcommission.org.uk/templates/search/document.cfm/6170>>.
- The Electoral Commission. (2002b). *Pilot scheme evaluation Crewe and Nantwich Borough Council 2 May 2002*. UK Government. Viewed 8 May 2006 <[http://www.electoralcommission.org.uk/files/dms/Crewe\\_Nantwich\\_6683-6235\\_\\_E\\_\\_N\\_\\_S\\_\\_W\\_\\_.pdf](http://www.electoralcommission.org.uk/files/dms/Crewe_Nantwich_6683-6235__E__N__S__W__.pdf)>.
- The Electoral Commission. (2002c). *Pilot scheme evaluation: St Albans City and District Council 2 May 2002*. UK Government. Viewed 8 May 2006 <[http://www.electoralcommission.org.uk/files/dms/StAlbans-final\\_6700-6250\\_\\_E\\_\\_N\\_\\_S\\_\\_W\\_\\_.pdf](http://www.electoralcommission.org.uk/files/dms/StAlbans-final_6700-6250__E__N__S__W__.pdf)>.
- The Electoral Commission. (2002d). *Public opinion and the 2002 electoral pilot schemes (NOP United Business World)*. UK Government. Viewed 8 May 2006 <<http://www.electoralcommission.org.uk/templates/search/document.cfm/6267>>.
- The Electoral Commission. (2003a). *The shape of elections to come: A strategic evaluation of the 2003 electoral pilot schemes. 2003*. UK Government. Viewed 8 May 2006 <<http://www.electoralcommission.org.uk/templates/search/document.cfm/8346>>.
- The Electoral Commission. (2003b). *Pilot scheme evaluation: St Albans City and District Council 1 May 2003*. UK Government. Viewed 25 September 2006 <[http://www.electoralcommission.org.uk/files/dms/StAlbans\\_PartA\\_10212-8261\\_\\_E\\_\\_N\\_\\_S\\_\\_W\\_\\_.pdf](http://www.electoralcommission.org.uk/files/dms/StAlbans_PartA_10212-8261__E__N__S__W__.pdf)>.
- Xenakis, A, & Macintosh, A (2001). Major Issues in Electronic Voting in the Context of the UK Pilots. *Journal of E-Government*, 1 (1). Viewed 8 May 2006. <<https://www.haworthpress.com/store/ArticleAbstract.asp?sid=J2PEME0LAA7A9L4PLLTG0NRMBLS3DU13&ID=50730>>.
- Weiner, E. (2004). 'The Bombay Ballot: What the US can learn from India's electronic voting machines'. *Slate*. Viewed 28 August 2006 <<http://www.slate.com/toolbar.aspx?action=print&id=2107388>>.