The Risks and Benefits of Electronic Voting

Dr Russell G. Smith, Senior Research Analyst - Australian Institute of Criminology
A paper presented at the 15th Australian Forum - Melbourne, 3 March 2001

Introduction

In both the public and private sectors there is a need to record people's views when decisions are made. Examples include choosing the office bearers of a club; casting votes at meetings of corporations or in parliamentary sittings; and choosing individuals to become members of parliament, or heads of government.

Achieving these objectives raises difficult practical issues where the votes of large numbers of people are to be recorded - although the principles are much the same whether one is recording votes from a five-member committee or the entire population of India.

This paper examines the benefits which digital technologies have in achieving these objectives; and considers whether they are able to do so better, in terms of meeting the above objectives, than the procedures that operate at present.

Current voting procedures and their problems

Throughout history a wide range of procedures have been devised to record people's votes. The ancient Greeks, for example, voted by acclamation or a clash of spears on shields. Other means of voting over the ages have included casting pebbles in ums, the division of crowds into groups, or balloting with shells, disks, or written papers (Sequoia Pacific Voting Equipment 1998). The introduction of secret ballots and the need for accountability required that new technologies be devised. These have included lever-operated machines, computer-readable punched cards, voting in enclosed cubicles at polling stations, and placing voting papers in locked or tamperproof boxes to ensure security. In order to prevent multiple voting, electors generally have their names crossed-off electoral rolls when they vote, or even have their fingers marked with slow-perishing ink. Finally, in order to enhance accountability, scrutineers observe all aspects of the voting process and numbers are sometimes recorded on voting cards so as to enable individual ballots to be recounted in the event of questionable practices being adopted.

Each of these procedures creates risks of fraud, abuse, and mistake and allegations have been made that various electoral procedures have been abused in the past (McGrath 1996; Copeman and McGrath 1997). Some of the problems include multiple voting; voting in the names of deceased or absent individuals; abuse of the postal voting system; and tampering with ballot papers - either by changing the marks on ballot papers, substituting fraudulent papers for legitimate ones, destroying papers, or adding additional papers to ballot boxes (see, for example, the abuses that took place in Richmond, Victoria, in 1978 (Grabosky 1989) and in New South Wales in 1987 (Patton 1988).

More recently, we have seen allegations of abuse in the registration of members of the Labor Party for pre-selection to seats in Queensland, which is currently being investigated by The Honourable Tom Shepherdson QC for the Criminal Justice Commission, Queensland (2000). Irregularities were also apparent in the means by which votes were counted in Florida during the United States Presidential Elections in 2000 (Manjoo 2000).

Others, however, have argued that the alleged abuses of the current system of voting, at least in Australia, have not been established and that the level of risk of abuse could not affect the outcome of an election in any event (Hughes 1998). Whether or not abuse has taken place, there is, arguably, room for improvement in a number of aspects of voting procedures, particularly those relating to enrolment of voters and the identification of voters at the time of casting their votes. There is also room for improvement in the laws that prohibit the many forms of electoral corruption which, in Australia at least, are variable across jurisdictions and contain widely disparate sanctions (Finn 1977).

Electronic Voting Procedures

Because of their facility in processing large amounts of information quickly, computers are seen by some as an effective solution to the problem of electoral fraud and abuse. Voting could take place from anywhere in the world with the results being recorded, analysed, and announced almost instantaneously. This would mean that Australian citizens resident in the United Kingdom, for example, could use the Internet to vote in Australian elections - thus avoiding the need to send approximately 18 tonnes of voting material to Britain when Australian federal elections are held (Mitchell 2000a).

Computers are now becoming all-pervasive in developed societies and governments, in particular, have determined to provide all appropriate services electronically within the next few years. In Australia, the Commonwealth hopes to achieve this objective by the end of 2001. Already we can obtain many government services electronically and obtain a vast range of government information from the Internet.

The Australian Electoral Commission (AEC) makes considerable use of information technology in carrying out its various activities that include conducting elections and referenda, maintaining the electoral roll, providing electoral information and educational programs to the public, and a number of other activities (Green 2000). At 30 June 2000, there were 12,430,851 electors enrolled on the Commonwealth electoral roll and during the year 1999-2000 the AEC processed 2,463,256 enrolment forms and amendments. The number of enrolled electors represented approximately 95 per cent of the eligible population at 30 June 2000.

In addition to maintaining the electoral roll in digital form, the AEC has an elaborate Website (http://www.aec.gov.au) which contains over 4,045 files of information and 25 links to other sites. The Homepage has information on Australian electoral history, a database of electorates, analysis of voting patterns, and other educational materials. The site is managed by eDIME under an outsourcing arrangement using MetaManage.

Computers have also been used in various aspects of voting systems around the globe for many years. The Swedish parliament, for example, first used electronic voting equipment in 1932, and electronic voting machines are now used in many countries around the world. These applications extend from simple electronic machines that record votes at polling booths, to on-line systems that enable voters to record their votes via the Internet and have them analysed entirely electronically. There are now many companies in the United States and Europe providing a range of electronic products in the form of hardware and software to facilitate electronic voting (see Cranor 2001 for a list of electronic voting technologies). One company even offers an electronic voting system designed for use by disabled voters (Hart InterCivic 2001).

A number of forms of computerised voting have been trialed or used overseas and in 1993, the various systems available for electronic parliamentary voting were examined by a team led by the Australian House of Representatives Speaker, the Honourable Stephen Martin MP (House of Representatives 1994). Although the report of these inspections was largely favourable, electronic voting in the Commonwealth parliament has not yet been introduced. In the ACT, however, the *Electoral Act* 1992 has been amended to permit a trial of electronic voting to take place at the forthcoming election to be held on 20 October 2001. The trial will not entail full Internet-based voting but rather the dual use of paper ballots and computers to assist in voting in four pre-poll voting centres and ten polling places. If this limited trial of electronic voting is successful, the ACT government plans to use Internet voting - with people voting from home - for the 2004 election (Armitage 2000, Green 2000, Mitchell 2000b).

Large corporations, such as Coles-Myer and NRMA have also begun to use on-line voting systems for shareholder meetings, principally in order to reduce the costs associated with paper proxy voting procedures and to increase shareholder participation in decision-making (Mitchell 2000a, Centenera 2001).

Computers are, of course, also used extensively in the private sector for business transactions. Substantial numbers of electronic transactions take place daily between consumers and financial institutions. Statistics complied by the Australian Securities and Investments Commission (2000), for example, show that there were 1,655,362,481 electronic funds transfer transactions conducted in Australia in the year 1999-2000. In the same period there were only 42 complaints made by consumers per million of those transactions.

Many of the same issues that face those who would seek to record votes electronically, also face those in the business world and, arguably, the solutions that will be deemed acceptable for financial institutions may also be

acceptable for the conduct of elections. In terms of the objectives outlined above, digital technologies have the following benefits and detriments.

Timeliness

Computers were designed specifically to enable data to be recorded and processed quickly and accurately. Accordingly, they have the capacity to record, to analyse, and to report the outcome of an election involving many millions of voters in a matter of minutes, if not seconds. In the study of the electronic voting systems used by a number of European parliaments, for example, it was found that voting took on average 30 seconds, whereas in the Commonwealth House of Representatives, divisions occupied between eight and nine minutes each. The use of an electronic system would, therefore have saved approximately nine hours a year for each member (House of Representatives 1994, p. 20).

The instantaneous processing of votes is not, however, always desirable and provision would need to be made for electors to have adequate time for reflection before casting their vote, and also for mistakes to be able to be rectified. The real-time public dissemination of the outcome of voting would also be undesirable as this could influence voting by those yet to cast their vote. This could be prevented by legislative bans being imposed on the publicity of the results of the election until voting actually closes. The result should then be able to be disclosed almost immediately.

A further difficulty concerning the rapid processing of votes relates to the data processing capacity of government servers and Internet Service Providers if an entire population of electors chose to vote at much the same time (Mitchell 2000a). Adequate computing capacity would need to be provided so that systems could handle the traffic. Alternatively, voting over a number of days could be permitted to prevent systems from being overloaded. In Australia, however, voters often leave voting to the last minute which could prove difficult to prevent. In addition, having voting available over a number of days would change political campaigning techniques that in the past have been directed toward a specific final polling day (Green 2000).

Accessibility

If Internet voting were adopted, many of the problems associated with postal voting would be overcome as electors located anywhere in the globe would be able to cast their vote in the same manner and at the same time.

A central practical difficulty, however, exists by reason of the need to provide every voter with access to a computer terminal, and for voters to be trained in making use of the relevant technologies. In Australia, at present, the Australian Bureau of Statistics has found that some 46 per cent of the adult population gained access to the Internet in the year to May 2000 - 6.4 million adults (Australian Bureau of Statistics 2006). This percentage would either need to be increased or else alternative means provided for electronic voting. Those who do not have access to a personal computer and modem at home or at work could, for example, vote at an Internet café which are beginning to become more readily available.

If electronic voting completely replaced paper voting, the financial savings made by the AEC could be re-directed to the establishment of voting terminals in remote locations in order to facilitate access, as well as to public education programs. The AEC might also need to establish a helpdesk and staff to offer assistance to those unfamiliar with computers. Alternatively, as Wireless Application Protocol (WAP) mobile telephones become more available, voting by mobile telephone may be used.

Secrecy and Deliberation

In many, but not all, voting contexts secrecy needs to be provided in order to ensure that voters do not suffer adverse consequences for having voted in a particular way. In conventional elections, individuals cast their votes in a polling booth that allows some degree of privacy when voting. Their votes are also anonymous - although the use of numbered ballot papers raises the possibility that individual votes could be traced back to particular electors.

If electronic voting were adopted, secrecy may either be enhanced or reduced. Voting using the Internet at home could be carried more privately and allow for greater deliberation than occurs currently at public polling

stations. In other situations, however, such as at a public Internet café or a crowded office space, privacy may be difficult to achieve. Voting in such circumstances could also under-emphasise the importance of the activity, or lead to undue influence being exerted on voters to vote in a particular way or to sell their vote for financial reward. In addition, concerns have been expressed that individual voting responses may be matched with individuals' identities, giving rise to the possibility of reprisals for having voted in a particular way (Green 2000). Arguably, appropriate internal controls within agencies that receive votes would prevent such abuse, while still allowing for matching to investigate voting irregularities.

Accuracy and Security

Computers are able to process information once entered with a great degree of accuracy, far better than can occur when people undertake clerical tasks manually. The recent difficulties found in the United States Presidential elections where ballot papers had to be re-counted illustrates the administrative problems and inaccuracies associated with counting ballot papers well (Manjoo 2000).

Digital technologies can also be designed to provide high levels of security through the use of encryption that makes it practically unlikely that encrypted data transmissions could be read and understood (Denning 1998).

There have, however, been numerous instances globally of computer networks in both the public and private sector being entered without authorisation and data altered or manipulated (see Grabosky and Smith 1998; Grabosky, Smith and Dempsey 2001). In one relevant case, a 24 year-old man in Brisbane gained access to and interfered with computer systems of the AEC, Australian Universities, and agencies in the United States such as NASA. He was convicted on 27 December 1996 and sentenced to three years' imprisonment and ordered to forfeit his computers and modems to the Commonwealth (Australian Federal Police 1997, p. 24).

Appropriate security measures such as firewalls and internal controls would need to be in place by the agency responsible for maintaining the electronic voting system and recording the election results. The provision of adequate back-up and storage facilities would also be essential to guard against accidental or deliberate loss of data (Schneider 1999).

On a more practical level, the physical protection of voters from intimidation also needs to be considered. By attending at a polling station in a public place, the risks of intimidation are reduced - although historical examples do exist of electors being compelled to vote in a particular way under threat of physical violence *(Borough of Cheltenham* (1869) 1 O`M. & H.62, in which a prize fighter was engaged on behalf of a candidate to intimidate voters). If voting were conducted at home or at some other private location, the risks of intimidation could be exacerbated and one could even imagine voters being compelled to enter a password or present a finger for scanning under duress in order for their vote to be manipulated. Whether this could take place on a wide enough scale to influence the outcome of an election is conjectural and, of course, such conduct would attract severe criminal penalties.

Authentication

The current procedures used to enrol electors and to identify them when voting are far from satisfactory and although the AEC seeks to maintain an accurate electoral roll, errors inevitably arise. In other contexts, the identification of members of the public for official purposes has proved to be similarly difficult. The Australian Taxation Office, for example, has encountered considerable problems in identifying with accuracy individuals and business entities to whom tax file numbers and Australian Business Numbers are issued. The Australian National Audit Office (1999) recently found that there were 3.2 million more tax file numbers than people in Australia at the last census; that there were 185,000 potential duplicate tax records for individuals; that 62 per cent of deceased clients had not been recorded as deceased; and that 40 per cent of de-registered companies were still recorded as active (see House of Representatives Standing Committee on Economics, Finance, and Public Administration 2000). Similar problems arise in the world of electronic commerce where financial institutions and merchants need to be sure of the identity of the person with whom they transact business (Smith 1999).

 The starting point in achieving authentication of individuals is the accurate registration of individuals through the submission of evidence of identification. This, if carried out carefully, permits the creation of a list of names

and other identifying information that correspond exactly with the individual in question. In terms of electoral processes, the maintenance of an accurate electoral roll lies at the heart of an efficient voting system.

At present an applicant for enrolment generally needs only to be 18 years of age or older, an Australian citizen, and to have lived at his or her current address for at least one month. The application form has also to be witnessed by someone who is already enrolled or entitled to be enrolled (see Part *VII, Commonwealth Electoral Act* 1918). Verification checks on the identity of the applicant are not regularly undertaken, although occasionally individuals are prosecuted for non-compliance with these requirements.

Abuse of the enrolment system was highlighted during a parliamentary inquiry in November 2000, when it was revealed that a pet cat by the name of 'Curacao Fischer Catt', was enrolled by her owner to vote in the New South Wales electorate of Macquarie in 1990 (Maiden 2000).

Identification of voters must also take place at the time they cast their votes. Some have suggested that voters be issued with cards, perhaps containing a signature and photograph, to improve ease of identification when voting. This, however, has been opposed on the grounds of cost and logistics as well as through concern that a voter's card would become the equivalent of a national identity card. Although a national identity card may, indeed, solve many of the problems associated with identification of individuals, it raises considerable problems relating to privacy and the security of information being held. In the United Kingdom, for example, a long and bitter struggle surrounded proposals to introduce a voluntary national system of identity cards used in conjunction with photo drivers' licences (Gill 1997).

The AEC already maintains an electronic electoral roll, but this is, of course, only as accurate as the information that is placed upon it. The AEC has, since the beginning of 1999, conducted a system known as Continuous Roll Update which includes data matching with information retained by other authorities and data mining of the electoral roll with the view to detecting fraudulent enrolments such as duplications or an unusually high number of enrolments.

The solutions that have been devised for the identification of individuals in the commercial world could be easily adapted for use in solving similar problems in the electoral system. There are four primary methods which may be used to authenticate a person's identity. Generally, these are based on: something that you have, such as a key or a plastic card (tokens); something that you know, such as a password or date of birth (knowledge); something related to who you are, such as your appearance, signature, or fingerprint (biometrics); or something indicating where you are located, such as your address and a corresponding telephone number (location). Risks of abuse arise with each of these approaches, although together they provide a reasonably secure system.

In a number of parliamentary voting systems in Europe, identification is established simply by the member being required to vote from his or her allocated seat - a rudimentary form of location-based identification. The potential exists, however, for members to sit in other members' seats and to cast votes which are then recorded in the name of the member to whom the seat has been allocated. Peer pressures within a small chamber would tend to ensure that this does not take place but in order to overcome this problem some parliaments now require members to use a smart card to identify themselves before casting their vote (House of Representatives 1994). Smart cards are, for example, used in the European Parliament in Brussels and in the United States House of Representatives. Of course, a smart card could be given to another member, in the same way as individuals could swap seats with one another in the chamber.

The use of a PIN or biometric authentication system may prevent abuses of this nature from taking place, although for national elections the secure delivery of a PIN to electors presents expensive logistical problems, similar to those that credit card issuers face when transmitting PINs to customers (Green 2000).

The most recent solution to the problem of authentication lies with the technologies of encryption. In Australia, the Commonwealth government has developed a strategy, entitled *Project Gatekeeper,* that aims to provide a common platform for the development of systems which rely upon public key cryptography and digital signatures. This strategy seeks to provide a system of secure electronic communications on public networks when dealing with Commonwealth government agencies. The policy behind *Project Gatekeeper* and the legal reforms contained in the *Electronic Transactions Act* 1999 (Cth) is that electronic communications should be treated in the same way for legal purposes as paper-based communications (functional equivalence). Any risks

of fraud and illegality should, therefore, be no greater in an electronic system than exist in paper-based systems (Australia, Office of Government Information Technology 1998).

In terms of the electoral system, *Project Gatekeeper* provides a starting point for both identification of voters and for security and verifiability of votes. It would also enable multiple voting by the same individual to be detected and enable the secure archiving of electoral data.

This system permits the parties to communications to have confidence that the person with whom they communicate is, in fact, who they represent themselves to be and that communications have not been altered once transmitted. The system also enables communications to be archived in secure storage facilities and every keystroke able to be reinstated for examination. Finally, each communication can be date and time-stamped in a secure way that cannot be altered. Such a system prevents individuals who gain unauthorised access to the network from reading or altering the communications in question. *Project Gatekeeper* has proposed that key pairs to be used in the Public Key Technology Framework would be issued to individuals who are able to establish their identity to an appropriate degree of assurance by supplying multiple and independent primary sources of identification such as those used to open a bank account.

The principal means by which fraud could be carried out in such a system would be for individuals to submit false documents to Registration Authorities in order to have cryptographic key pairs issued to them for use in fraudulent ways. Alternatively, there is the possibility that key tokens, which would take the form of smartcards, could be stolen and used without authorisation by compromising their security features. Access may also be gained illegally to cryptographic keys which are stored on personal computers or servers unless appropriate risk management measures are in place.

These are, however, relatively remote risks that would require a considerable degree of organisation and planning on the part of those seeking to compromise the system. Arguably, these risks are considerably more remote than the risks of fraud that arise under the present electoral procedures.

Verifiability

One of the main concerns with electronic voting is the possibility that data may be manipulated once a vote has been registered.

Traditionally, electoral systems have sought to establish verifiable paper audit trails so that allegations of fraud may be investigated and those responsible prosecuted. One important feature of the Australian electoral system is that numbers are placed on ballot papers that correspond with the voter in question so that an audit may be conducted if the electoral process is disputed. Although this could, and has, led to disclosure of how an individual has voted, its benefits in terms of allowing auditing are said to outweigh the risk of infringement of secrecy (see Hughes 1998, p. 491, n. 40).

The need for an evidentiary audit trail also exists in commercial transactions where the parties involved need to establish that electronic messages have not been interfered with or others substituted. As organisations in both the public and private sectors move toward so-called dematerialised systems - in which no paper records are kept of electronic communications at all - so the need to verify transactions will become of critical importance.

The public key encryption systems, such as that contemplated in *Project Gatekeeper*, provide a range of procedures to ensure that electronic communications cannot be interfered with and that enduring audit trails exist. The use of so-called hashing algorithms, for example, provides an assurance that a digital data transmission once received matches exactly that transmitted, and digital signatures ensure that communications are able to transmitted securely and confidentially. If adequate security protocols are followed in establishing the system, it should operate at least as securely than the existing paper-based system - and hopefully much more securely. To achieve this outcome, it will be necessary to avoid any infrastructure weaknesses, while at the same time ensuring that security protocols are adhered to.

Conclusions

On the basis of the available evidence, it appears that electronic voting systems - if introduced using appropriate technologies - could reduce the risks of voting fraud that occur under existing systems.

Electronic voting using public key encryption technologies would provide a secure system as long as adequate procedures were in place to ensure that cryptographic key pairs were issued only to individuals who establish their identity to an appropriately secure degree. This would mean that organisations would need to enhance their procedures substantially in registering voters, perhaps even requiring some form of biometric identification to be used before a key token were issued.

As the federal government moves towards the digital age in which paper trails of evidence will no longer be maintained, it will become imperative for the electoral system to make use of these technologies as well.

Their use may even enhance the democratic process by enabling plebiscites to be conducted more often and at less cost than under our present system in which a single referendum can cost many millions of dollars (see Firkin 2000).

Those who have expertise in electoral fraud need to work closely with those who will design electronic voting systems to ensure that the problems that have arisen and been solved in the past, no not re-emerge in the future, and that any new risks are kept to a minimum.

References

Armitage, L. 2000, 'Electronic Voting Wins Bipartisan Assembly Support', *Canberra Times,* 28 November.

Australian Bureau of Statistics 2000, *Use of the Internet by Householders, Australia,* February and May 2000 editions (Cat. No. 8147.0), Australian Bureau of Statistics, Canberra.

Australian Federal Police 1997, *Annual Report 1996-97,* Australian Federal Police, Canberra.

Australian National Audit Office 1999, *Management of Tax File Numbers,* Audit Report No 37, 1998-99, Performance Audit, ANAO, Canberra.

Australian Securities and Investments Commission 2000, *Complaints Made Under the EFT Code of Conduct 1999-2000,* ASIC, Sydney.

Centenera, J. 200 1, 'Assembly's Electronic Election Stirs Interest', *Canberra Times, 10* February, p. C4.

Copeman, C. and McGrath, A. 1997, *Corrupt Elections.. Recent Australian Studies and Experiences of Ballot Rigging,* Towerhouse Publications, Kensington, NSW.

Cranor, L. F. 2001, 'Electronic Voting Hot List', http://www.research.att.com/-lorrie/voting/hotlist.html (visited 28 February 2001).

Criminal Justice Commission, Queensland 2000, *Inquiry into Allegations of Electoral Fraud,* http://www.cjc.qld.gov.au (visited 28 February 2001).

Denning, D. 1998, 'Cyberspace Attacks and Countermeasures', in Denning, D. E. and Denning, P. J. *Internet Beseiged.. Countering Cyberspace Scofflaws,* ACM Press, New York, pp. 29-55.

Finn, P. D. 1977, 'Electoral Corruption and Malpractice', *Federal Law Review, vol.* 8, pp. 194230.

Firkin, H. 2000, 'Electronic Polling: Government By the People', *The Age (Melbourne),* 25 July, p. I.T. 1-13.

Gill, M. 1997, 'Ethnic Minorities and Policing: The Impact of National ID Cards', *Security Gazette, vol.* 39, no. 8, p. 33.

Grabosky, P. N. 1989, *Wayward Governance: Illegality and its Control in the Public Sector,* Australian Institute of Criminology, Canberra.

Grabosky, P. N. and Smith, R. G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities,* Federation Press, Sydney / Transaction Publishers, New Brunswick.

Grabosky, P. N., Smith, R. G., and Dempsey, G. 2001, *Electronic Theft: Crimes ofAcquisition in Cyberspace,* Cambridge University Press, Cambridge.

Green, P. 2000, 'The Internet and the Electoral Process' in *The Politics of the Future: The Internet and Democracy in Australia,* 5 October 2000.
http://search.aph.gov.au/search/Parllnfo.ASP?action=view&item=59&resultsID=zUnG9 (visited 27 February 2001)

Hart InterCivic 2001, 'eSlate Direct Record Electronic Voting System', http://www.hartis.com/ (visited 26 February 2001).

House of Representatives 1994, *Electronic Voting: Report of Inspection on Equipment Used in the Parliaments of Belgium, Denmark, Finland, Sweden and the United States ofAmerica and in the European Parliament Building in Brussels,* Parliament of the Commonwealth of Australia, Canberra.

House of Representatives Standing Committee on Economics, Finance and Public Administration 2000, *Numbers on the Run: Review ofthe ANA 0 Report No. 3 7 1998-99 on the Management of Tax File Numbers,* Parliament of the Commonwealth of Australia, Canberra.

Hughes, C. A. 1998, 'The Illusive Phenomenon of Fraudulent Voting Practices: A Review Article', *Australian Journal of Politics and History, vol.* 44, no. 3, pp. 471 - 9 1.

Maiden, S. 2000, 'Curious Case of a Cat With the Right to Vote', *The Advertiser (Adelaide),* 16 November, p. 4.

Manjoo, F. 2000, 'Ballots Need an Up-Grade', http://www.wirednews.com/news/politics/0, 1 283,40078,00.htmI (visited 10 November 2000).

McGrath, A. 1996, *The Frauding of Votes?* Tower House Publications, Kensington, NSW.

Mitchell, S. 2000a, 'On the E-Hustings', *The Australian, 1* August, p. 53.

Mitchell, S. 2000b, 'Electronic Voting', *The Australian,* 14 November, p. 33.

Office of Government Information Technology 1998, *Gatekeeper: A Strategyfor Public Key Technology Use in the Government,* Australian Government Publishing Service, Canberra.

Patton, D. 1988, 'The Great Vote Scarn', *The Optimist,* June/July, pp. 12-15. f,

Schneider, F. B. (ed.) 1999, *Trust in Cyberspace,* National Academy Press, Washington.

Sequoia Pacific Voting Equipment 1998, 'History of the Voting Machine', http://www.spve.com/ (visited 26 February 2001).

Smith, R. G. 1999, 'Identity-Related Economic Crime: Risks and Countermeasures', in *Trends and Issues in Crime and Criminal Justice,* No. 129, Australian