AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 224

Electronic Voting: Benefits and Risks

Russell G. Smith

New areas of fraud have been high on the research agenda of the Australian Institute of Criminology for some time. While much of our research has focused on the difficult issues to do with financial fraud, electoral fraud can also have serious ramifications for the government and the community.

Recent investigations into electoral matters, such as the inquiry conducted for the Criminal Justice Commission in Queensland (as it then was), have raised many criminal justice issues to do with the conduct of ballots. The integrity of an electoral system is a fundamental bulwark against corruption and the ability of organised groups within the community to misuse democratic institutions for improper purposes. New technologies can both assist and hinder those wishing to perpetrate electoral fraud.

Already many trials have taken place of electronic voting procedures in both the private and public sectors in an attempt to reduce costs, improve voter participation and enhance efficiency in conducting ballots. In the Australian Capital Territory, the Legislative Assembly election held on 20 October 2001 allowed some voters to cast their votes using computers located at polling stations in order to enhance the efficiency of the ballot process. But will electronic voting be subject to the same problems of security and manipulation that have occurred in the context of business transactions? This paper tests the effectiveness of electronic voting against eight essential requirements that any electoral process needs to satisfy in order for elections to be conducted both freely and fairly in modern societies.

Adam Graycar
Director

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.

The essential requirements for such activities to be conducted freely and fairly are:

- the need to record information and to have the results available quickly (*timeliness*);
- the need to have a system that is accessible to all and easy to use (*accessibility*);
- the need to ensure secrecy of what takes place (*secrecy*)—except where open elections are called for;
- the need for voting to be undertaken seriously, after due deliberation (*deliberation*);
- the ability to ensure that each individual's vote is recorded and counted accurately (*accuracy*);
- the need to guard against manipulation and interference with information once recorded (*security*);
- the need to ensure that individuals cannot be impersonated (*authentication*); and
- the need to verify what has taken place through the use of traceable information trails (*verifiability*).

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

April 2002

ISSN 0817-8542
ISBN 0 642 24261 5

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

five-member committee or the entire population of India.

This paper examines the benefits that 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. It also considers how crime and corruption in the electoral process can be minimised through the use of computerised voting procedures. In order to focus the discussion, this paper will primarily examine parliamentary voting procedures within Australia, rather than voting in private sector organisations and within parliamentary chambers.

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 urns, the division of crowds into groups, or balloting with shells, disks or written papers. In more recent times, some countries developed lever-operated machines, computer-readable punched cards, voting in enclosed cubicles at polling stations, and placing voting papers in locked or tamper-proof boxes to ensure security—not always with success, however. In order to prevent multiple voting, electors in some countries have their names crossed off electoral rolls when they vote, while others are required to have their fingers marked with slow-perishing ink—a technique never adopted in Australia. Finally, in order to enhance accountability, scrutineers in many countries observe all aspects of the voting process.

Each of these procedures creates risks of fraud, abuse and mistake. In Australia, allegations have been made by some groups that various electoral procedures have been abused in the past (McGrath 2001). Some of the alleged 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]). On occasions, those involved in such abuse have been prosecuted and imprisoned for breach of the many criminal offences set out in Australia's Electoral Acts (see Finn 1977).

More recently, the conviction of three individuals for fraud relating to the registration of members of the Australian Labor Party for preselection to seats in Queensland led to inquiries by:

- the Queensland Criminal Justice Commission (2001)—now the Queensland Crime and Misconduct Commission—by the Honourable Tom Shepherdson QC;
- the Queensland Legislative Assembly's Legal, Constitutional and Administrative Review Committee (2000); and
- the Commonwealth Parliament's Joint Standing Committee on Electoral Matters (2001).

The focus of these inquiries was on inaccuracy and maladministration of electoral rolls, which often lies at the heart of fraud. It was concluded by these various investigations that the cases of enrolment fraud in Queensland could not have affected the results of any parliamentary elections, state or federal. Although the management of the electoral rolls by the Australian Electoral Commission (AEC) was not found to be at fault, and widespread and organised electoral fraud in order to affect the results of federal elections was not uncovered, various administrative improvements and amendments to electoral law were recommended (AEC 2001a).

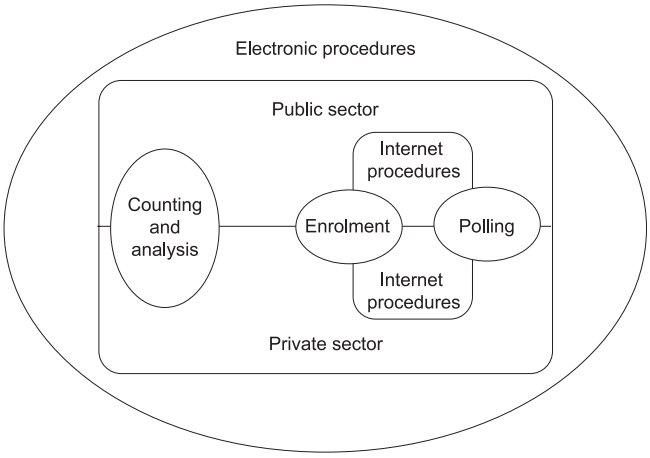
The AEC has argued that the alleged abuses of the current system of voting in Australia have not been established and that the level of risk of abuse could not affect the outcome of an election in any event (Hughes 1998; AEC 2001b). Whether or not abuse has taken place, there is, arguably, room for improvement 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.

Electronic Voting Procedures

Computers have been used in various aspects of voting procedures around the globe for many years now. They have application in both public and private sectors and facilitate the processes of enrolment of voters, as well as the casting, counting and analysis of votes (see California Internet Voting Task Force 2000). As shown in Figure 1, Internet technologies form only one component of the electronic voting environment.

The Swedish parliament 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 online systems that enable voters to record their votes via the Internet and have them analysed entirely electronically. There are now many

Figure 1: *The electronic voting environment*



companies in the United States and Europe providing a range of electronic products in the form of hardware and software to facilitate electronic voting.

A number of forms of computerised parliamentary voting have been trialled or used overseas and, in 1993, a team led by the Australian House of Representatives Speaker, the Honourable Stephen Martin MP (House of Representatives 1994) carried out an inspection and review of a number of systems. Although the report of these inspections was largely favourable, electronic voting in the Commonwealth Parliament has not yet been introduced.

In the Australian Capital Territory (ACT), however, the election of the Legislative Assembly held on 20 October 2001 entailed a trial of electronic polling at four pre-poll voting centres and eight polling places, as well as the use of computer-assisted counting of ballots. Voters at designated polling stations were given the option of using a card that could be swiped at a terminal in an enclosed cubicle, and then voting through the use of a personal computer and keyboard to navigate around and select their candidates. Votes were recorded by the computer and security precautions ensured that voters could not vote twice: the barcode on the card could only be used once. Informal votes could be recorded and votes could not be altered once entered because the keystrokes could be compared with what appeared on the screen.

Although the system trialled in the ACT required the *Electoral Act 1992* (ACT) to be amended, cost over $400,000 and had some minor technical problems—such as barcode readers not always operating efficiently—it greatly facilitated the voting procedure and enabled the result to be known more quickly than in the past (Lucas 2001).

The AEC and the other state and territory electoral authorities also make considerable use of information technology in carrying out their various activities. The Commonwealth electoral roll—which at 30 June 2001 recorded the names of 12,555,142 electors—is maintained by computer, and this made the task of processing the 2,624,229 enrolment forms and amendments that were lodged in 2001 considerably easier than if a paper roll were used. In addition to maintaining the electoral roll in digital form, the AEC has an elaborate web site which contains over 4,000 files of information and a considerable number of links to other sites (AEC 2001a).

Large corporations, such as Coles-Myer and NRMA, have also begun to use online 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 2000, Centenera 2001).

Timeliness

Computers were designed specifically to enable data to be recorded and processed quickly and accurately. Accordingly, they have the capacity to record, analyse and 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 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 closed. The result should then be possible to disclose 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 2000). Even in the ACT trial of electronic voting, the capacity of servers led to some difficulties being encountered. Adequate computing capacity would therefore 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, the logistical difficulties 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. 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 2000).

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. The Australian Bureau of Statistics has found that some 50 per cent of the adult population gained access to the Internet in the 12 months to November 2000—6.9 million adults (Australian Bureau of Statistics 2001). 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 Internet cafés, which are becoming more numerous.

If electronic voting completely replaced paper voting, the financial savings made by the AEC could be redirected 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 anonymously in a polling booth that allows a degree of privacy when voting.

If electronic voting were adopted, secrecy may either be enhanced or reduced. Voting using the Internet at home could be carried out privately and allow for greater deliberation than occurs currently at some public polling stations. In other situations, however, such as at a public Internet café, a crowded office space—or indeed in a family room at home—privacy may be difficult to achieve, with voters being subject to pressure or even coercion from friends or family to vote in a particular way, or even to sell their vote for financial reward. Voting in such circumstances could also under-emphasise the importance of the activity and, of course, would mean that political parties would no longer be able to supply how-to-vote cards at polling stations in the hope of influencing undecided voters. 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 with a great degree of accuracy—far better than occurs when people undertake clerical tasks manually. The difficulties found in the United States' presidential elections in 2000, where punch-card ballots had to be recounted, 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 highly unlikely for encrypted data transmissions to be read and understood.

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. In one case, a 24-year-old man in Brisbane gained access to and interfered with computer systems of the AEC, various Australian universities, and agencies in the United States such as NASA. He was convicted on 27 December 1996, sentenced to three years' imprisonment and ordered to forfeit his computers and modems to the Commonwealth (Australian Federal Police 1997, p. 24).

Often these cases arise because adequate security measures, such as firewalls and internal controls, are not in place, thus enabling either insiders or external hackers to gain access to systems. The provision of adequate backup and storage facilities would also be essential to guard against accidental or deliberate loss of data.

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 (see *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.

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 of the Commonwealth's *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).

The starting point in achieving authentication of voters is the accurate registration of individuals through the submission of evidence of identification. In terms of electoral processes, the maintenance of an accurate electoral roll lies at the heart of an efficient voting system.

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 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 pressure 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 used, for example, 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 that individuals could swap seats with one another in the chamber.

The use of a personal identification number (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 solutions that are being devised for the identification of individuals in the commercial world could be 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 for reasonable security.

The most recent solution to the problem of authentication lies with the technologies of public key cryptography and digital signatures. Although the global implementation of public key technologies in the private sector has been retarded due to cost and inability to agree on uniform standards, the Commonwealth Government in Australia has developed a strategy, entitled *Project Gatekeeper*, that aims to provide a secure system of electronic communications on public networks when dealing with Commonwealth government agencies (Office of Government Information Technology 1998). Already some large Commonwealth agencies are making use of public key systems to secure electronic transactions. 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 communicating parties 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 can 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 smart cards, could be stolen and used without authorisation by compromising their security features. Access may also be gained illegally to cryptographic keys that 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. 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—the need to verify transactions will become of critical importance.

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 "hashing algorithms", for example, provides an assurance that a digital data transmission, once received, matches exactly the one transmitted. Digital signatures ensure that communications can be transmitted securely and confidentially. If adequate security protocols are followed in establishing the system, it should operate at least as securely as the existing paper-based system—and hopefully much more so. 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.

Conclusion

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 arise 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 established 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 was issued.

As the Federal Government moves towards a digital age in which paper trails of evidence will no longer be maintained, it will become feasible 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. The 2001 federal election, for example, was estimated to cost $107.8 million, including some $68 million paid to the Australian Electoral Commission (Dodson 2001).

Those who have expertise in electoral fraud need to work closely with the designers of electronic voting systems to ensure that the problems that have arisen and have been solved in the past do not re-emerge in the future, and that any new risks are kept to a minimum.

Acknowledgments

The ACT Electoral Commissioner, Mr Phillip Green, provided helpful comments on an earlier draft of this paper, as did the Australian Electoral Commission and an anonymous reviewer. This final version remains, however, the responsibility of the author.

References

Australian Bureau of Statistics 2001, *Use of the Internet by Householders, Australia, November 2000 edition*, cat. no. 8147.0, Australian Bureau of Statistics, Canberra.

Australian Electoral Commission (AEC) 2001a, *Annual Report 2000–2001*, Australian Electoral Commission, Canberra, http://www.aec.gov.au (visited 12 December 2001).

—— 2001b, *Electoral Fraud and Multiple Voting*, AEC Backgrounder, no. 14, 24 October, http://www.aec.gov.au/pubs/backgrounders/vol_14/main.htm (visited 12 December 2001).

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

California Internet Voting Task Force 2000, *A Report on the Feasibility of Internet Voting*, California Secretary of State, Bill Jones, Sacramento, http://www.ss.ca.gov/executive/ivote/ (visited 13 December 2001).

Centenera, J. 2001, "Assembly's electronic election stirs interest", *Canberra Times*, 10 February, p. C4.

Dodson, L. 2001, "Price of the vote tops $100m", *The Age* (Melbourne), 5 December, p. 1.

Finn, P.D. 1977, "Electoral corruption and malpractice", *Federal Law Review*, vol. 8, pp. 194–230.

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

Green, P. 2000, "The Internet and the electoral process", in *The Politics of the Future: The Internet and Democracy in Australia*, 5 October 2000, online text: 523123, http://search.aph.gov.au (visited 6 April 2002)

House of Representatives 1994, *Electronic Voting: Report of Inspection on Equipment Used in the Parliaments of Belgium, Denmark, Finland, Sweden and the United States of America and in the European Parliament Building in Brussels*, 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. 471–91.

Joint Standing Committee on Electoral Matters 2001, *User Friendly, Not Abuser Friendly: Report of the Inquiry into the Integrity of the Electoral Roll*, Parliament of the Commonwealth of Australia, Canberra.

Legal, Constitutional and Administrative Review Committee 2000, *The Prevention of Electoral Fraud: Interim Report*, no. 28, Queensland Legislative Assembly, Brisbane.

Lucas, S. 2001, "Despite glitches, electronic voting 'a success'", *Canberra Times*, 25 October, http://www.canberra.yourguide.com.au/detail.asp?class=News&story_id=100005&subclass=local&m=10&y=2001 (visited 6 April 2002).

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 upgrade", http://www.wirednews.com/news/politics/0,1283,40078,00.html (visited 10 November 2000).

McGrath, A. 2001, *The Frauding of Votes?* H.S. Chapman Society, Sydney.

Mitchell, S. 2000, "On the e-hustings", *The Australian*, 1 August, p. 53.

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

Patton, D. 1988, "The great vote scam", *The Optimist*, June/July, pp. 12–15.

Queensland Criminal Justice Commission 2001, *The Shepherdson Inquiry: An Investigation into Electoral Fraud*, http://www.cjc.qld.gov.au/netscape/ALLPUBLICATIONS.html (visited 3 April 2002).

Dr Russell G. Smith is Deputy Director of Research at the Australian Institute of Criminology

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.

Project no: 0040