Overhauling Australian Democracy: The Benefits and Burdens of Internet Voting

BRYAN MERCURIO*

The right to vote for parliamentary representatives is at the heart of Australian democracy. Election officials expend great effort and care ensuring that the person voters prefer in an election actually wins the election. But ensuring the will of the people and the corresponding victory of the duly elected parliamentarian is not the only consideration in the electoral process, as public confidence in the electoral system and the results it produces is of equal importance. In order for democracy to flourish, public confidence in the electoral system must remain strong. Voters must have confidence that the system will work as designed and without major fault. For this reason, electoral change is often slow and deliberate instead of swift and reactionary.

On the other hand, modern life has recently wholeheartedly embraced technology. The accessibility, relative low cost and seemingly endless capabilities of the Internet has rapidly expanded the medium beyond our recent imagination. By the late 1990s, every major political party maintained a website to disseminate information and communicate directly with supporters.[1] More recently, home computer ownership and Internet use has risen exponentially,[2] and more than 4.2 million Australians can now do a variety of time-consuming tasks,

* Faculty of Law, University of New South Wales, and Director, Electoral Law Project at the Gilbert + Tobin Centre of Public Law. The author would like to thank Professor George Williams, University of New South Wales, and Graeme Orr, Griffith University, for their helpful comments on an earlier version of this article. The author would also like to thank the Electoral Council of Australia, whose generous support made this project possible.

1 See Rachael Gibson and Stephen J Ward, 'Virtual Campaigning: Australian Parties and the Impact of the Internet' (2002) 37(1) *Australian Journal of Political Science* 99.

2 The World Wide Web expanded from 50 servers in 1993 to over 100 000 in 1997. See Ari Staiman, 'Shielding Internet Users from Undesirable Content: The Advantages of a PICS Based Rating System' (1997) 20 *Fordham International Law Journal* 866, 874. As of March 2002, the Internet had over 560 million users (a number expected to grow beyond 762 million by 2003). See *Global Internet Statistics* (2002) Global Research <http://www.glreach.com/globstats> at 27 August 2002.

such as banking, shopping for clothes or groceries or paying bills, online in a matter of seconds.[3]

The potential to use the Internet to conduct elections is now embraced by some as necessary to voting 'customers', who increasingly demand more convenience within the electoral system.[4] After initial scepticism, politicians and electoral officials in numerous countries initiated discussion and support for the idea. While their response to the pressure may have been simply an attempt to satisfy the constituency, using the Internet to improve the electoral process seems like a logical, natural extension of the burgeoning technology. In fact, despite our inclination to treat the electoral process with judicious care, the leap to technological advances is not that remote, as federal, State and local governments now rely on the Internet to provide their constituencies with essential governmental information and interactive services online.

Moreover, a system of computerised, electronic voting ('e-voting') would appear to have several advantages over the traditional form of voting. A perfected computerised system of voting would seem to be a secure, cost effective, efficient, convenient, environmentally friendly way to vote. In addition, the total electoral breakdown suffered in the 2000 United States Presidential election proved that traditional methods of paper voting are not infallible.[5] For these reasons, many nations, including Australia, have determined that the time is ripe to study Internet voting and consider ways to introduce computerised voting into the voting electorate.[6]

3 As of September 2002, over 4.2 million Australians subscribe to Internet services and more than 9.2 million adults (66 per cent of the adult population) had accessed the Internet during the 12 months to November 2000. See Australian Bureau of Statistics, *Use of the Internet by Householders, Australia* (2001) <http://www.abs.gov.au/Ausstats/abs%40.nsf/e8ae5488b598839cca25682000131612/6445f12663006b83ca256a150079564d!OpenDocument> at 8 November 2002; Australian Bureau of Statistics, *Internet Activity, Australia* <http://www.abs.gov.au/Ausstats/abs@.nsf/e8ae5488b598839cca25682000131612/6445f12663006b83ca256a150079564d!OpenDocument> at 15 January 2003.

4 An American study revealed 61 per cent of younger voters are 'enthusiastic' about voting online. See *Six Out of Ten Young Voters Say Yes to Internet Voting*, Business Wire <http://www.votehere.net/content/press/990723.asp> at 2 May 2001.

5 For a complete review of the 2000 United States Presidential election, see *Elections Central: A History of Presidential Elections* <http://www.multied.com/elections/> at 8 January 2003; *CNN: 2000 Election Archive* <http://www.cnn.com/ELECTION/2000/> at 8 January 2003.

6 The Australian Capital Territory ('ACT') Electoral Commission Annual Report 1999/2000 states that the 2001 offline e-voting trial 'would be the first step to a wider use of technology for voting at future elections, including the possibility of

On the other hand, governments cannot leap into the technological unknown when elections are involved. The election of parliamentarians is the foundation of Australian democracy. Not only is maintaining the integrity and accuracy of the election process essential to our thriving democracy, but the electoral system also needs the public to trust, understand and have the utmost confidence in the system by which we elect our parliamentarians. If citizens were to lose confidence in the electoral process, the nation would lose its credibility, honour, and, ultimately, its democracy.[7] For this reason, even the 2001 Australian Capital Territory ('ACT') Legislative Assembly elections, which allowed voters at certain pre-poll voting centres and polling stations to cast their vote using an offline form of electronic voting, generated heated debate and extensive commentary. Discussion regarding online voting generates even more comments, misconceptions, questions and fears.

This article explores and evaluates the potential benefits and burdens of introducing a system of online voting to the electoral process, with a detailed analysis of the two most popular e-voting options: remote Internet voting and Internet voting at the polling station. Because the terms 'Internet voting' and 'e-voting' are often misunderstood and/or misused, part one defines these terms within the context of this article. In order to clearly understand electoral issues, part two briefly describes the criteria needed in order to conduct a successful election. Part three introduces remote Internet voting and Internet voting at the polling station. Part four analyses the barriers to and benefits of implementing Internet voting in the electoral process. Part five reviews and evaluates Internet voting experiences from the United States and the United Kingdom. Part six explores the legal implications arising from a move to implement Internet voting in Australia. Part seven recommends further study of the issue and puts forward several proposals leading to the gradual introduction of Internet voting into the Australian electoral landscape.

Internet voting'. See ACT Electoral Commission, *Annual Report 1999/2000*, 2 <http://www.elections.gov.au/annualreport2000/anrep00a1.html> at 15 May 2002. See also Colin Barry et al, *Electronic Voting and Electronic Counting of Votes: A Status Report* (2001) 9 <http://www.eca.gov.au/reports/electronic_voting.pdf> at 15 May 2002. (The Australian Electoral Commission report, produced in conjunction with the Victorian Electoral Commission, assesses various forms of electronic and Internet voting). Moreover, the recently enacted *Electoral Act 2002* (Vic) s 100(2) provides for e-voting at overseas or interstate early polling centres.

7 For constitutional considerations involving voting and sovereignty, see George Williams, *Human Rights under the Australian Constitution* (2002) 155-97.

What is Electronic Voting?

The term 'electronic voting' lacks clear definition and is often used with conflicting meanings. The term can be used broadly to describe any form of mechanical voting, such as punch card machines or voting at the polling station using a computer terminal or any similar touch screen or mouse activated machine that stores votes and may or may not have the ability to tabulate votes. These forms of e-voting are not online forms of voting, meaning the systems are not connected to Internet lines and there is no chance of outside interference (for example, hackers). This article will not discuss offline e-voting, instead, this article's focus is on Internet-based online voting and the benefits and burdens thereof.

Confusion exists even within the terms 'Internet voting' or 'online voting' as well, as the terms are often misunderstood/misused and the cause of much confusion. These terms have become synonymous with remote Internet voting when in fact they could mean any form of voting on the Internet, whether at home, the polling station, voting kiosk, or any other place in which the Internet is accessible. As the benefits and burdens of Internet voting depend upon which version of Internet voting is on offer, this article will differentiate between and clarify which form of Internet voting is being discussed.

Criteria for a Successful Election

There are several fundamental aspects to a free and fair election. Accordingly, the aspects listed below are necessary to, and must be satisfied in order to hold, a successful election.

- Authentication and eligibility – only authorised and eligible voters should be allowed to cast a ballot;
- Accuracy – votes should be recorded and counted correctly, ensuring the will of the people is represented;
- Uniqueness – voters should only be allowed to cast one ballot;
- Integrity – votes that are forged, modified or deleted should be detected;
- Verifiability and auditability – verification that all the votes have been accounted for in the final tally and that reliable and authentic records exist to this effect;
- Reliability – election systems should ensure against the loss of any votes, even when faced with electoral failures;
- Secrecy and non-coercibility – voting should be done in secret without voters ever having to reveal how they cast their ballot;

- Flexibility – election equipment should allow for a variety of platforms and technologies and be accessible to all voters, including those with disabilities;
- Convenience – voters should be able to quickly cast their ballot without undue delay;
- Certifiability – election systems should be regularly tested and certified to ensure against electoral failure;
- Transparency – voters should possess a general understanding of the voting process and should not be deceived into voting a certain way; and
- Cost-effectiveness – election systems should be affordable while still being efficient and effective.[8]

In order to ensure free and fair elections, any new voting measure must satisfy the above criteria. It is equally important to consider how new election systems meet other aspects of democracy, such as access by demographic groups, election logistics and administration, deliberative and representative democracy, and the political culture of elections in Australia. Moreover, as this article later reflects, the above 'necessary' criteria interact with such 'aspects of democracy', as each change in the voting system offers trade-offs and balances between the various values. For instance, a move to increase security in the voting process would increase the costs of running an election and reduce voter convenience and flexibility. Likewise, a move to encourage participation and the franchise could lead to a reduction in authentication and verifiability.

Internet Voting Systems

Australians put their faith in free and fair elections, therefore, the electoral process must get it correct the first time, every time. While e-commerce accepts that between 5-10 per cent of all Internet transactions are the result of credit card fraud, such a level of fraud would

[8] This criterion was compiled from a White House commissioned report operated by the US National Science Foundation, the Internet Policy Institute and the University of Maryland. The report was the product of an October 2000 workshop, where political scientists, computer scientists, election officials and others analysed and assessed the feasibility of Internet voting and identified research priorities for the advancement of Internet voting: Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda* (2001) 11 <http://www.internetpolicy.org/research/results.html> at 11 January 2003. For a similar set of criteria, see Colin Hughes, 'Institutionalizing Electoral Integrity' in Marian Sawer (ed), *Elections: Full, Free and Fair* (2001) 142-57.

fundamentally undermine an election.[9] Even a small hiccup in a voting system could cause irreparable harm to the Australian electoral system and democratic process. The 2000 United States Presidential election proved that minor procedural deviations combined with electoral oversight could quickly turn an advanced electoral and democratic system of a highly sophisticated nation into a tangled fiasco. With this background in mind, electoral commissions considering implementing online e-voting have two very distinct forms to consider:

Remote Internet Voting

Remote Internet voting allows the voter to cast their ballot in the comfort of their own home, at the Internet café or wherever the Internet is accessible. Proponents of remote Internet voting envision a voter logging on to the voting website via secure means, establishing their identity, and then voting in a real-time transaction at any time convenient to the voter on election day. This formula is simple to understand and similar to any other web-based transaction.

The convenience and undemanding nature of remote Internet voting has generated excitement from the media as well as the voting electorate. Remote Internet voting will be the most difficult form of e-voting to implement, however, and cost, security and policy-related issues must be more adequately addressed before its implementation.[10]

9 See Ed Gerck, 'From Voting to Internet Voting' (2000) 1 *The Bell* 5 (Gerck estimates that 10 per cent of transactions are the subject of fraud); Craig Bickenell, *Credit Card Fraud Bedevils Web*, Wired News <http://www.wired.com/news/business/0,1367,18904,00.html> at 5 April 2001. (Bickenell states 5-6 per cent of Internet transactions are fraudulent).

10 Remote Internet voting depends on a number of factors outside the electoral officers' control, such as whether the voter's operating system is supported by the proper voting and encryption software, whether the voting system is able to recognise that the person attempting to vote is a legitimate voter who has not previously voted in the election, and the influences of persons present who may influence, compel or coerce a voter to vote in a certain way. It is not hard to imagine a situation where a voter feels compelled to vote a certain way due to influences of other people in the area where the person is voting, such as other family members, friends, co-workers, etc. Even more frightening is the scenario where voters are voting under duress or coercion, such as a supervisor urging the employee to vote in a certain way under the threat of sanction.

Internet Voting at the Polling Station

While the long-term promise of remote Internet voting is great, the short-term reality sees another Internet-based option, Internet voting at the polling station, as a more viable alternative. Polling booth voting is similar to the existing forms of voting, but instead of the voter casting their ballot with a pencil and paper, they instead use a computer terminal connected to a central server.

In terms of satisfying the keys to a successful election, this option is practical and appealing, as it offers greater convenience and efficiency over traditional voting while also allowing election officials to maintain control over the computer operating system, as well as monitor and control the physical surroundings of the venue, making the security risks more manageable and the risk of electoral failure significantly less than with remote Internet voting. While voters would not have the convenience of voting away from the polling station, they would obtain numerous benefits from e-voting at the polling station, such as fast and simple voting, as well as quicker election results. Election officials would also benefit from Internet voting at the polling station, as Internet voting would add efficiency and diminish the current administrative burden associated with traditional voting. Officials could also use Internet voting at the polling station as an evolutionary system towards remote Internet voting.

E-voting at the polling station appears similar to the processes voters know and trust. Voters would appear at the polling station on the requested day and have their names marked off the roll as normal, before retiring to a booth which, instead of being equipped with paper and pen, would have a terminal connected to a closed network server at which voters could cast their ballots electronically. The computer would then forward the votes via modem to a central location for counting and collating.[11]

Additionally, as election officials maintain control over the infrastructure and environment, voting at the polling station provides as much guarantee of authentication and privacy as traditional paper voting. Internet voting at the polling station would also eliminate the possibility of anyone voting more than once under the same name, as

[11] The vote forwarding process would occur either during the election or after polling closes. For instance, the system could 'store and forward' the voting data by secure means to the central server during the election to prevent flooding and data loss if the communication lines fail. Conversely, the computer could record and store votes in a localised server at each polling station before sending the final count via secure connection to a central server.

the computer system would not allow multiple votes. This system is not without its drawbacks, however, as the short-term cost of an e-voting system would be substantial and the benefits to voters not nearly as significant as remote Internet voting.

Voting Barriers and Benefits

Potential Barriers

Technological Problems

Several technologies are used in an attempt to ensure authentication, secrecy and security of Internet voting systems. These security measures include encryption technology (the scrambling of information during transmission) and electronic signatures (the use of passwords, personal identification numbers ('PIN'), biometrics, digital signatures, etc) to verify a voter's identity and maintain the integrity of the data.

At present, there are several technical barriers that will have to be removed before any form of online voting could be implemented. First and foremost, technological measures need to be upgraded to ensure the accuracy and the integrity of an election. In addition, the e-voting system designed to implement online voting must be protected from interruption and security breaches, such as those that might occur from a hacker or a clogged network connection.

Security breaches have the potential to irreparably damage an election. Technical security breaches can occur through two ways: (1) by an attack that targets the client or server directly, commonly called a penetration attack; or (2) by an attack that targets and interrupts communication between the client and the server, commonly called denial of service.[12]

User and the Server

Penetration attacks occur when a hacker transports a virus to its target by one of a variety of mediums, including floppy disk, CD-ROM, download, e-mail or by exploitation of an existing bug or security flaw in the targeted computer or browser. Penetration attacks are a common occurrence and difficult, if not impossible in some cases, to de-

[12] For a detailed analysis of Internet security considerations, see Avi Rubin, *Security Considerations for Remote Electronic Voting Over the Internet*, AT&T Labs-Research <http://avirubin.com/e-voting.security.html> at 11 January 2003.

fend against.[13] Once the virus is transported and in place, the hacker can do as they please and could easily spy on a user casting their ballots, prevent the user from casting their ballot, or even modify a voter's ballot.[14] Even worse, the hacker can accomplish all of the aforementioned activity without the knowledge of the voter or detection from security measures, such as encryption devices or anti-virus software.[15] A virus targeting an election and released on election day would cause untold damage to the sanctity of the secret ballot, as well as the integrity of the election.

A successful remote Internet voting system must also protect against a plethora of other hacker activities, including 'man in the middle',[16] 'page jacking',[17] or similar disruptive and highly damaging attacks that could be aimed at voters on election day.[18] These types of attacks pose the same risks as other infiltration attack methods, yet are much

13 Ibid 2-3. Hackers routinely damage, delay or delete information flowing over the Internet. There have been numerous well-documented instances where hacking has played havoc with the computer systems of major companies, including Yahoo, Hotmail and United States government sites. See The Center for the Study of Technology and Society <http://www.tecsoc.org/> at 8 January 2003. In Australia, a Brisbane man was jailed for two years after causing serious environmental harm when he caused raw sewage to flow into creeks and parks in 2001: *Computer Hacker Jailed for Two Years*, ABC News Online, 31 October 2001 <http://www.abc.net.au/news/state/qld/archive/metqld-31oct2001-15.htm> at 11 January 2003.

14 A trojan horse virus can be activated at any time after delivery, including remotely, by timer, or by the detection of certain events by the host (or a combination of the above).

15 Encryption devices are powerless if hackers can gain access to the system before the devices commence protection. Moreover, even if the device successfully commences protection, this kind of attack usually targets an area of the computer that is not protected (encryption protects only the operating system and browser). Anti-virus software is ineffective because the hacker codes the program to gain access and then effectively 'authorises' the computer to make the changes it dictates. See Internet Policy Institute, above n 8, 13-14.

16 'Man in the middle' occurs when a hacker misleads the user into thinking they are on the correct website when in fact they are on the hacker's site. The hacker collects the information entered by the user for later fraudulent use while the user believes they have successfully completed their business on the proper site.

17 'Page jacking' occurs when a hacker leads a user off the intended website and onto an impostor website. Once on the impostor site, the user's browser is disabled and the user is shown advertising or other information. The user then has some difficulty in accessing their intended website due to the blocks presented by the hacker.

18 One example of another method used by hackers is 'spamming', which floods the system with requests to prevent the authorised user from responding to legitimate requests.

easier to carry out, and even the most advanced encryption technologies cannot guarantee success against a potential breach.[19]

Some experts feel the security concerns associated with Internet voting from open network computers, as would occur in remote Internet voting, cannot be overcome without significantly decreasing the perceived benefits of remote Internet voting, namely, convenience for the voter. Such measures to add security to the remote Internet voting process could include having voters pre-register for online voting, sending a CD-ROM to voters to install, and/or sending voters a password and PIN number.[20]

Internet voting at the polling station would be less susceptible to outside hacker attacks and considerably safer than remote Internet voting due to the fact that election officials control the server and voting software at the polling station. With reliable technology and support to administer the voting system, the system can easily be configured to prevent Internet communication with any outside server, as well as prevent any disgruntled worker from installing any additional software onto the machines.[21]

Denial of Service

Election officials must also ensure the path between the user and server is secure. Providing a secure transmission requires an authenticated line between the user and server as well as the encrypted transportation of data along this line. Current technologies can ensure the latter through encryption technology (such as public key infrastructure ('PKI')), however, maintaining the authenticated communication link between user and server cannot be guaranteed.

Therefore, denial of service attacks focus on the path between the computer user and the server. A hacker effectuates the attack by overloading a website with requests for information, thus 'jamming' the lines and preventing others from using the site.[22] Currently, there is no way to stop the 'jamming' without shutting down the system, and thus shutting out legitimate users until the diagnosis and network

19 Internet Policy Institute, above n 8, 16.

20 Richard M Schum, *Internet Voting: Its Perils and Promise*, Internet Policy Institute, 5 <http://www.netvoting.com> at 9 May 2002.

21 As opposed to the open system used in remote Internet voting, online polling station voting uses a closed network system, where the voter's interface is not accessible remotely, thereby eliminating the threat of online hacker attacks. See ibid 2.

22 In addition, daemons can be installed on a user's computer, without that user's knowledge, to perpetuate the attack against a server or site.

administration is completed. Before implementing Internet voting, election officials must ensure the path between the computer user and the server cannot be illegally breached.

Moreover, election officials must be able to guarantee with some certainty that the centralised computer server will be able to effectively handle the amount of Internet traffic created by large groups of people attempting to vote at the same time. This problem, commonly referred to as a 'bottleneck', is similar to jamming, except that it occurs by an overwhelming number of legitimate users. As many Internet websites get millions of hits per day,[23] this aspect of remote Internet voting should not be too much of a concern with proper technical support.[24]

Even though the likelihood of denial of service attacks and bottlenecks on polling station voting is minimal, the threat can be avoided entirely by designing a system that allows voting to continue even if the line of communication between the precinct and the server is lost. In essence, to ensure the system is safe, the computer switches to a direct recording electronic ('DRE') mode without losing a vote, meaning votes are recoverable even if the online system were corrupted beyond repair.[25] Unfortunately, this fallback-system of DRE is only compatible with Internet voting at the polling station, as it is not feasible to implement DRE on every remote computer.[26]

[23] One of the most visited Internet websites, CNN, gets 230 000 hits per minute on a slow day and can get more than 2 million hits per minute during breaking news: *CNN Delivers Unprecedented Online Service*, Volera <http://www.volera.com/corporate/pressroom/casestudies/cnn.html> at 8 January 2003.

[24] Some commentators claim the 'traffic' problem can be avoided by allowing voting over multiple days. While this system effectively operates with postal voting, multiple-day voting has the potential to affect significantly the political advertising campaign of the parties and may lead to situations of bribery or votes for favours (see below).

[25] DRE essentially operates as an offline, computerised e-voting system, where votes are recorded, stored and tabulated electronically. For more analysis of offline e-voting, see Bryan Mercurio, 'Electronic Voting: Benefits and Burdens' (Paper presented at the 2002 Electoral Law Conference, Sydney, 6 December 2002).

[26] Leaving aside the financial and logistical costs of implementing DRE on personal computers, it would be unacceptable for election officials to rely on voters to store and transmit their vote in the event of a denial of service attack. Thus, in remote Internet voting, the reliability of the communication between the computer and the server, as well as maintaining a functioning back-up server, is much more critical.

Compatibility

While the issue of system compatibility has long been a problem for programmers, it is particularly acute when considering remote Internet voting due to the high standards of security and fairness required during an election. While a standardised system could easily be developed and instituted for use at the polling station, the issue is quite complex in regards to remote Internet voting. Internet voting issues revolve around such questions as: which platform(s) will the system be able to run on, which operating systems will support it, which browsers will be compatible with the system, and which language should the ballots be formatted in?

Fairness and equality dictate that a system compatible with all common web browsers be used in order to present a system accessible to all voters who attempt to vote remotely over the Internet. However, a system compatible with multiple systems adds to the complexity, cost and timeliness of the system, as it would have to be constantly updated, re-configured and re-tested to account for continuous evolution and improvements in the various platforms.

Balancing the Interests

The inherent risks associated with Internet voting create a fundamental trade-off between the convenience for the voter and the security of the voting system. As convenience is added to the electoral process by allowing people to vote remotely, security of the vote is reduced; as well, as security increases (by such measures as smart-card readers, biometric authentication devices and cryptographic devices), much of the convenience associated with Internet voting dwindles.

The task of election officials developing, controlling and maintaining a properly functioning and secure site to allow Internet voting is certainly feasible, but quite daunting. In fact, the California Internet Task Force declared there are 'significant' technological threats to the security, integrity and secrecy of Internet voting, but went on to conclude that the Internet could be used to develop a system that would be at least as secure from vote-tampering as the current absentee ballot process.[27] Commentators have suggested numerous different formats to overcome the obstacles to implementation of a remote Internet voting regime, all of which have numerous positives as well as obvious drawbacks. Two such methods are outlined below.

[27] California Secretary of State, *California Task Force on Internet Voting* (2000) 1 <http://www.ss.ca.gov/executive/ivote> at 7 May 2002.

One method would require the voter to encrypt the ballot with a secret key before sending it to the election office.[28] The voter would send the ballot, with their blind signature, to a verifier who verifies that the person is a registered voter. If found to be valid, the ballot would be returned to the voter, who would remove their identification signature and send the ballot, with the encrypted signature of the validator, electronically to the electoral office. The electoral office would then publish the names of Internet voters for those voters to verify that they were the ones who actually voted. The voter then sends the encryption key to the electoral office and the electoral office publishes the encrypted ballot and key for vote verification.

Another possible remote Internet voting solution would be to have voters sign up to vote remotely before the election. The electoral office could send those voters a disk containing a cryptographic key and an affidavit, which voters would sign and return.[29] The encrypted key would only be activated after the affidavit is checked against the voter's name on the roll. The actual vote would also be encrypted with a different key to generate an anonymous email.

Both of the above examples would provide voters the chance to cast their ballot from anywhere in the world. Both examples also attempt to provide security by adding layers of protection-related actions required by the voter. In doing so, both examples limit voter convenience and add significant administrative costs to the election.

Voter Sabotage

Election officials recognise that Internet voting at the polling station lends itself to the possibility of security failure and malfunction during the election and have acted accordingly. For instance, the ACT trial implemented numerous security measures to protect the integrity of the election, such as bar-coded swipe cards to prevent voters from voting multiple times. While these measures can prevent some voter fraud, they cannot prevent all forms of voter destruction. While the risk of voter sabotage is slight, destructive acts, such as a voter smearing gel on the screen in an attempt to disable the machine or

[28] The Commonwealth government could aid in this process, as it developed a key cryptography process for identity verification (*Project Gatekeeper*) in an attempt to provide secure transmissions within government agencies. See the National Office for the Information Economy <http://www.govonline.gov.au/projects/publickey/Gatekeeper.htm> at 8 January 2003.

[29] The disk would be secure so that it could not be numbered to track the voter and how they voted.

alter votes, could burden election officials and volunteers and may even delay voting.

While some commentators point to the potential destructive acts of voters as evidence of the unsuitability of the voting method, further study regarding potential tampering reveals this argument to be nothing more than a red herring. Not only is such behaviour not expected out of the Australian voter, but, in the event of tampering, it would be on such a small scale as to not affect the election results. Moreover, if the e-voting system allowed voters the opportunity to check which candidates they have voted for before registering the vote, the malfunction could be corrected without losing or altering a single vote. Commentators have had success with this argument in swaying the public against the technology, but in reality, no system is safe from the intentional destructive acts of voters. Yes, a voter could smash or otherwise disable an e-voting machine, but, just as easily, a voter could light a match and drop it into the ballot box and destroy paper votes. While both are possible, neither is likely.

That said, while media reports slamming e-voting are overblown and often incorrect or misleading, the slight risk of election day failure or corruption is present. Offline e-voting elections have experienced problems such as the machine's screen failing to light up, malfunctioning from repeated finger jabbing, or barcodes failing to activate machines. These problems are rare and easily discovered. In most elections, problem machines are usually corrected within minutes of discovering the problem and very rarely does a machine have to be decommissioned during an election. A properly calibrated and well-maintained machine rarely suffers a total breakdown, and, to the author's knowledge, has not resulted in votes being lost.

In any event, election officials must establish an emergency back-up plan to prepare for the worst. In order to avoid contested elections and lawsuits, the system must be tested against error and an easily assembled back-up plan must be generated and put in place in the event of system failure.

Audit Trail

The verifiability and accountability of the election result is essential to maintaining the confidence of the electorate. Any voting system, whether traditional or electronic, must ensure that all votes have been accounted for in the final tally and that reliable and authentic records exist to this effect. Complicating the matter is the fact that the electoral system must also ensure that the voter's choices remain secret.

The paper trail for verification, commonly called the 'audit trail', is removed from all forms of e-voting (online and offline), as e-voting trusts computers to record properly, forward and tabulate the votes. This situation potentially creates problems in cases of close election results or when allegations of mismanagement or fraud occur. Even if e-voting is proven to be 100 per cent accurate, it lacks the tangible proof, and therefore the reassurance, some people need in order to trust the election results.

Moreover, even though e-voting companies insist their polling place systems prevent against vote loss, and therefore creates an audit trail, by sending and burning every transaction on the server to a CD, which would serve as a back-up in the event of a hardware problem or total malfunction, voters may view this claim with suspicion.[30] Voters are familiar with and accept the painstakingly long process of manually counting and re-counting ballots in order to reach an election result. Even though the manual system is fraught with error, the removal of a paper audit trail coupled with the possibility of an e-voting breakdown may raise an unacceptable level of risk in the electorate. Consequently, some voters will oppose e-voting simply because they insist upon physically seeing the results of an election.

Internet voting at the polling station has the ability to resolve the problem and create an audit trail by having the machine print out a paper ballot which the voter would place into a special voting box. If need be, election officials could check the accuracy of the system by manually counting the paper ballots. This satisfies the need for some to have a paper trail and also allows election officials to closely scrutinise the voting system. On the other hand, it also increases administration time and costs. For this reason, this precaution, if adopted, should probably only be used in trials and phased out as voters grow confident in the technology. A similar system, yet more cost-effective and practical, is in operation in Brazil, where the entire election is now conducted using offline ATM-style e-voting technology.[31] In Brazil, after a voter completes the voting process, the machine prints a receipt located behind a plexiglass covering which the voter can view. The voter can then see which candidates the machine has reg-

[30] The companies also assert that the randomising algorithm in their systems mix up the ballots so they are not stored on the server in chronological order, thus ensuring the vote of each voter cannot be traced back to that person: Barry et al, above n 6, 9.

[31] Brazil phased in e-voting, first implementing it in local elections (1996) before introducing it to most federal electorates (1998) and finally the entire population (2002). See Brazilian Electoral Office <http://www.tse.gov.br> at 9 January 2003.

istered the votes for and allows voters to cancel out votes and vote again if necessary.[32]

Unfortunately, such a system is not available in remote Internet voting and there is no way presently known to create a paper trail during remote voting, short of attempting to have every voter print a receipt and send it to a central location. Quite obviously, such a system is not feasible for any number of reasons.

Costs

The cost of initiating any form of Internet voting is considerable. For instance, in a system of Internet voting at the polling station, election officials would expend a significant amount of time and resources designing, evaluating or purchasing an e-voting system. A substantial amount of money would also be spent on purchasing computer equipment for each polling station. Moreover, more resources would be needed to train staff and to hire technical experts to monitor the accuracy, security and effectiveness of the system. In total, the start-up cost of producing a reliable and secure online e-voting system would run into the multi-millions, a figure that could possibly be prohibitive.[33]

Developing a remote Internet voting system will be an even more time-consuming and expensive venture. The initial outlays of developing or purchasing a reliable and safe remote e-voting system, hiring technical experts to monitor the system and training staff in the new system would be significant, if not prohibitive.[34] In addition, significant resources would need to be dedicated to maintaining the accu-

[32] Approximately 3 per cent of the paper ballots are checked against the machine recorded votes to ensure the accuracy of the system: Holli Riebeek, *Electronic Voting in the Amazon*, IEEE Spectrum, November 2002 <http://www.spectrum.ieee.org/WEBONLY/wonews/oct02/brazil2.html> at 27 November 2002.

[33] Estimates on the cost of implementing online e-voting are around US$20-$50 million per county in the United States: Lance J Hoffman, *Internet Voting: Not Ready for Prime Time (Yet)* 4 <http://www.cpi.seas.gwu.edu/library/presentations.php> at 15 January 2003. Without a detailed survey, there is no way to accurately calculate the cost of an Australian move to Internet voting.

[34] For instance, the state of Washington task force stated digital signature technology provided the most secure form of remote Internet voting, however, the technology was deemed too expensive to provide: Derek Dictson and Dan Ray, *The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections*, White Paper (2000) 4 <http://www.securepoll.votingpaper.com> at 5 November 2002.

racy and integrity of the system, as well as upgrading the system at regular intervals.

Equal Access

Another barrier to implementing Internet voting may be issues of equality and equal access, as some argue that Internet voting could deny the right to equality to, and/or unfairly disadvantage, some groups in the community. While the arguments are stronger in non-compulsory voting jurisdictions, the arguments can also be made in Australia.

While it is true that every potential voter could not vote electronically, the traditional methods of voting also exclude many people with disabilities from voting without assistance. In fact, various forms of online and offline e-voting systems used or trialed in numerous countries, including Australia, the United States, the United Kingdom and Japan, have been praised for their ease of use and guidance for voters.[35] E-voting has also been well-received by elderly and disabled voters and appears to allow some voters, including blind voters, the opportunity to vote without assistance for the first time in their lives.[36]

However, the above assumes the voter is voting at the polling station instead of remotely voting via the Internet. Even though some dis-

[35] See, for example, Barry et al, above n 6, 4; Internet Policy Institute, above n 8, 25 (advancing the proposition that poll site e-voting allows more people with disabilities access to voting than any other form of voting).

[36] See Department of the Parliamentary Library, *Electronic Voting in the 2001 ACT Election*, Research Note 2001-02, No 46, 18 June 2002. Previously, blind voters would have to vote with the assistance of election officials, but the voice instructions through disposable headphones provided by the e-voting system allowed these voters to finally vote in secret. The fact that some disabled voters are unable to vote without assistance under traditional forms of voting, and thereby denied their right to vote in secret, even though technology exists to allow these voters to vote in secret, may violate the *Disability Discrimination Act 1992* (Cth) or similar State statutes. The issue has been litigated in the United States (District of Columbia) under a similar statute (*Americans with Disabilities Act 1990*). The case settled, with the electoral commission agreeing to make available a certain number of e-voting machines at each polling station. See American Association of People with Disabilities, *AAPD Plaintiff in a Landmark Lawsuit Against the District of Columbia that has Just Been Settled* <http://www.aapd-dc.org/docs/landmarksettledcvotemach.html> at 5 January 2003; Perry Bacon, 'Optical-Scan Ballot Debuts for Primary', *Washington Post* (Washington), 5 September 2002, DZ03. While one can argue that the *Disability Discrimination Act 1992* (Cth) *may* not allow such lawsuits, the issue has not been tested and can be debated. In addition, such a high profile suit, even if unsuccessful, would be highly embarrassing to the Electoral Commission and may have the capability to force change in this way.

abled voters, particularly blind voters, use computer programs that aid their unassisted home computer use, it may not be feasible or cost-effective to produce software that allows every voter to cast their ballot remotely. Therefore, election officials must have e-voting systems operating at the polling station to fully realise the benefits of Internet voting for the elderly and disabled.

Other social science issues also imply that remote Internet voting will not be able to fully replace the polling station. For instance, if remote Internet voting has a lower rate of informal votes, as studies seem to suggest, then people without access to remote Internet voting would be disadvantaged. If it can be shown that a certain segment of the population are disadvantaged by this disparity, then the system of Internet voting could be challenged as offending policies of equality and equal access.[37] As long as remote Internet voting is an alternative to, and not a replacement of, polling station voting, election officials should avoid fundamental inequities that remote Internet voting could produce.[38]

Political Culture

For many Australians, the act of voting by ballot is an ingrained part of the democratic process. Australians celebrate and have confidence in an electoral system that has stood the test of time and repeatedly proven its merits in the electoral process. While it is true that a growing number of ballots are cast in pre-poll centres or by post instead of at the polling station, the act of families gathering at a polling station, and maybe stopping by the sausage sizzle on the way to casting their ballot, is a deeply entrenched symbol of democracy in Australia. Australians know, understand and have confidence in the current system of voting. They appreciate the complexity of the process while understanding the simplicity of the act of voting.

The ritualistic celebration of democracy and liberty seen at a polling booth is something not to be discarded lightly. A move to online voting, therefore, would have to be done in such a way as to not undermine the community spirit that has developed on election day. For

[37] People with Internet access are, for the most part, highly educated, young and live in urban areas. Regardless of the rate of informal votes, in countries without compulsory voting, remote Internet voting could add an extra incentive encouraging those groups with Internet access to vote, which could be seen as a fundamental inequality, as voting results would be affected by the change in voting patterns of one voting demographic.

[38] This assumes a sufficient number of polling stations remain open to accept voters and that voters are not disadvantaged by the length of travel to each station.

these reasons, many commentators advocate the introduction of Internet voting as an alternative to traditional voting, as opposed to a replacement of the traditional voting system.[39]

While social science issues are more abstract than security or cost-related concerns, the effect of Internet voting on the community is a burden to its implementation. Although Internet voting at the polling station would have a minimal effect on the voting culture,[40] the advent of remote Internet voting on a widespread scale could affect the voting culture quite substantially.

Opposition to remote Internet voting claim its implementation has the potential to destroy the social cohesion of Australian voters and produce the negative result of a divided society. Traditional voting is seen to promote the community over the individual, where the civic duty of voting is dutifully followed by all citizens, citizens who for one moment in time enjoy equal standing to all others, regardless of situation, wealth, colour, beliefs or education. On the other hand, if one segment of society opts to vote remotely instead of physically going to the polling station, the community's ideal voting forms are seen to disappear. For these reasons, a move to online voting would have to be done in such a way as to not diminish or undermine the significance of the event and the sense of community voting creates.

Other social arguments against remote Internet voting generally revolve around the idea that remote Internet voting could trivialise and under-emphasise the meaning and importance of the event. Some opponents insist that voters will not give adequate thought to their choice or to the magnitude of the event if they do it at home, work or in the Internet café. As many voters have a fair idea of the issues and their preferred candidates before entering the polling station, the fact that a keyboard and screen is in front of them instead of a pencil and paper does not alter the fact that the person still must actively decide who to tick (or number, as the case may be) before they leave the corridor.[41] In fact, proponents of Internet voting insist the contrary is

[39] See California Secretary of State, above n 27. The report deemed it not legally, practically or fiscally feasible to develop a remote Internet voting system that would completely replace traditional voting. See also Barry et al, above n 6, 16.

[40] Voters would still travel to the polling booth to vote, but would vote via a computer terminal or touch screen machine as opposed to a pencil and paper. However, any form of voting needs to have the voters' confidence, meaning issues regarding computer tabulations, malfunctions and the lack of an audit trail (all of which were discussed earlier) would figure into the issue of voting culture.

[41] Moreover, an effective e-voting system should allow for people to check their ballot before sending it through (ie placing it in the box). This mechanism for

true, that voters will sit down to vote and use the Internet to research the candidates and the issues before selecting their preferred choices.[42] While the truth may lie somewhere in between the two opposing views, it seems unlikely that remote Internet voting will have a dramatic effect on views regarding the importance of the event or on the way Australians cast their ballots.

The effect of remote Internet voting on the election campaign is another area that concerns many commentators. Some advocates claim remote Internet voting could possibly allow voters to cast their ballots over several days, instead of the traditional one-day period. They claim a multiple-day voting period would add convenience to the process and reduce the likelihood of Internet traffic causing server delays. While the necessity of multiple-day voting is open to debate, multiple-day voting would significantly alter the political election campaign.

Political campaigns are designed to end with the culmination of a one-day election, and multiple-day voting could forever change the landscape of advertising.[43] One can imagine the situation of a party in a close election almost begging people to vote for them on the last day of voting with unrealistic promises. One can also imagine groups of individuals or communities holding out their votes, swapping votes or selling votes until promised what they desired. The fiasco this situation could turn into is almost comical until one remembers that we are dealing with the values and principles of Australian democracy.

Another potentially major change to political campaigns resulting from Internet voting regards the distribution of 'how-to-vote' cards. At present, supporters hand out cards listing the political party's (and other interested groups') partiality for particular preferences. These cards, deemed 'how-to-vote' cards, are often relied on by voters, who

checking the ballot could simply be done by a pop-up box appearing which states something of the following nature: 'You voted for X. Are you sure you want to vote for X? If Yes, click ENTER. If No, click BACK.'

42 Of course, the Internet gives virtually anyone with a computer the opportunity to 'publish'. Thus, while information is plentiful on the Internet, the quality and consistency of information is often inconsistent and unreliable.

43 Phil Green, 'The Politics of the Future: The Internet and Democracy in Australia' (Paper presented at the Australian Political Science Association's Politics of the Future Seminar, Canberra, 5 October 2000).

vote in the manner requested by their party of choice via the cards.[44] Voters who choose to cast their ballot remotely via the Internet will lose the benefit of receiving the cards before voting. Although there could be a procedure for pre-registered cards to be available to the Internet user, and most Internet voters would likely take up the option, viewing the cards via the Internet may not have the same appeal or effect as viewing the paper-based card at the polling booth. Moreover, being physically handed a card at the polling station is yet another one of those events, such as the smell of the sausage sizzle, that makes voting day a celebrated event.

Another potential question arising from remote Internet voting is to what extent advertising or on-screen electioneering would be allowed or tolerated. Would the voting website have links to the party websites? If so, to all the parties or just the major ones? Would the election website sell advertising or allow parties' pages to outline their campaign promises or smear the other side? These are but a few of the many questions that would need to be discussed, studied and answered before remote Internet voting could be introduced on a wide-scale basis.

Finally, opponents of remote Internet voting claim that the use of Internet technology will alter the existing structure of Australia's deliberative democracy.[45] The federal framework of Australia, complete with the separation of powers, sufficient checks and balances against the arms of the government and a bicameral legislature, quite deliberately promotes deliberation over efficiency and substantially limits the excesses of direct democracy. The advent of remote Internet voting could substantially undermine the system, as the Internet could be seen as an end run to the legislative process and be used to overcome logistical and economic barriers to more frequent elections or referenda. Politicians could threaten the integrity and character of the Australian system of government by seeking to please the electorate or avoiding tough decisions by referring the issue to referendum. This process of direct democracy could lead to frequent referenda as opposed to genuine reflection and would not serve the best interests of Australians.

[44] For more on how-to-vote cards, see *How-To-Vote Cards and their Importance*, Australianpolitics.com <http://www.australianpolitics.com/elections/htv/> at 9 January 2003; Australian Electoral Commission, *Voting* <http://www.aec.gov.au/_content/What/voting/index.htm> at 9 January 2003. Note, there are no how-to-vote cards in the ACT.

[45] Schum, above n 20, 9.

Potential Benefits

Convenience

Proponents insist Internet voting would add needed convenience to the democratic process of electing parliamentarians. Voters out-of-town on polling day would simply have to log on to the Internet to vote, dispensing with the hassle of having to apply for a postal vote and hoping it arrives.[46] In addition, voters would no longer have to balance work, family or other commitments with their responsibility to vote.

Internet voting at the polling station would also reduce the time burden on the busy Australian voter. Currently, the average Australian takes eight to nine minutes to cast their ballot for the Commonwealth House of Representatives, while voters using offline e-voting systems in various European parliaments only take an average of 30 seconds to vote.[47] While the complex ballots of the Australian election could hardly be completed in as little as 30 seconds, the difference is quite striking and does show how e-voting can save time and shorten queues on election day.

In addition, a well-designed e-voting system is extremely user friendly. While traditional voting currently gives voters the right to choose between a few languages, e-voting can accommodate as many different languages as required without adding significant cost to the system. As stated earlier, e-voting also provides some disabled voters the opportunity to finally cast a ballot without assistance from electoral officials.[48]

Moreover, e-voting has proved popular with mainstream voters. Statistics show that voters who have used various online and offline e-voting systems in Australia, the United States, Japan, the United Kingdom and continental Europe overwhelmingly rate e-voting very

[46] Internet voting would particularly suit the busy professional called out-of-town at short notice and unable to apply for a postal vote.

[47] House of Representatives, Parliament of the Commonwealth of Australia, *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* (1994) 20. See also Russell Smith, 'Electronic Voting: Benefits and Risks' (2002) No 224 *Trends and Issues in Crime and Criminal Justice* 3.

[48] See Department of the Parliamentary Library, above n 36.

highly and uniformly praise the ease of use, speed and assistance provided by the system.[49]

Fewer Polling Stations and Less Administration

While the author believes polling station voting should always remain an option for the numerous reasons stated earlier, the number of polling stations needed during an election could be significantly reduced if a substantial proportion of the voting population chose to cast their ballot remotely. Therefore, in the long run, Internet voting could see the government spend less on voting infrastructure and administration.

Moreover, remote Internet voting would dramatically reduce, if not eventually eliminate, the need for overseas Australians to use the postal vote. This simple change would also have a positive environmental effect as Australia currently sends approximately 18 tonnes of material relating to elections to Britain alone during election campaigns![50]

Even simply allowing Internet voting at the polling station would ease the administrative burden election officials currently face, as e-voting would eliminate much of the paper voting by-product. In addition, the responsibility of election monitors, and also the threat of lost ballots, would decrease as monitors would no longer have to carefully supervise the safety and security of the ballots, and instead could concentrate on other pressing matters that inevitably arise on election day.

[49] In Riverside, California, the offline touch screen technology used for voting recently received over a 99 per cent approval rating: Farhad Manjoo, *The Case for Electronic Voting* (14 November 2000) Wired News <http://www.wired.com/news/politics/0,1283,40141,00.html> at 5 January 2003; NOP Research, *Public Opinion in the Pilots* (2002); *Electronic Voting Trial 'A Success'* (28 June 2002) ACT Electoral Commission <www.elections.act.gov.au/adobe/2001ElectionReviewComputerVoting.pdf> at 15 January 2003 (reporting that 89 per cent of e-voters found it easy to use and understand). While a University of Maryland study (Centre for American Politics and Citizenship, *An Evaluation of Maryland's New E-Voting Machines* (2002) <http://www.capc.umd.edu/rpts/MD_EVoteEval.pdf> at 15 January 2003) reported that one-in-six Maryland voters needed assistance with e-voting in that state's recent election, the study fails to assess the abundance of assistance voters need under the current system. See Thad Hall, *LA Story: The 2001 Election* <www.reformelection.org/data/reports/la-hall.pdf> at 5 January 2003 (reporting that countless non-English speaking Americans in Los Angeles required assistance to vote with a paper ballot).

[50] Smith, above n 47, 3.

Minimise Informal Votes

Trials in several countries prove e-voting systems produce a much lower percentage of informal votes than traditional voting. In most e-voting systems, the rate of informal votes is negligible, compared with the large rate of informal votes that exist under other forms of voting.[51] This low rate of informal votes is due to the design of e-voting systems, which attempt to ensure the voter properly casts their ballot by leading the voter through the process and confirming that the selections the voter made are the ones they intended to make.[52]

In addition, e-voting takes the risk of human error or bias, as seen clearly in the 2000 United States Presidential election, out of the equation. The inconsistent, unbalanced system of recognising and discounting informal votes seen in this election could not be repeated in a computerised system of voting.

Fast, Accurate Results

A computer has the ability to record and report data immediately after receiving it into its system or at the end of the polling period. International e-voting evidence proves that e-voting can significantly shorten the counting process,[53] and evidence from the offline ACT trial shows the system made no distribution errors when distributing preferences.[54]

The Australian electoral system would benefit more than most from e-voting, as the e-voting system would distribute preferences automatically and eliminate the time-consuming process of manual counting, and allow for election results to be known much more quickly than under the present system. In fact, a recent parliamentary paper stated e-voting results in greater accuracy and speed in the dis-

51 For example, in Riverside, California, where touch screen voting is used, the rate of informal votes is negligible, compared to its former system using punch cards, which resulted in a large number of votes for multiple candidates: Manjoo, *The Case for Electronic Voting*, above n 49. The offline ACT trial resulted in an informal rate of 0.57 per cent, compared with 4.32 per cent of paper votes being deemed informal. In comparison, informal votes were cast on 4.32 per cent of the ballots in the 1998 election and 6.24 per cent in 1995: Department of the Parliamentary Library, above n 36, 1.

52 Some voters often use the ballot as a form of protest, so the system must be designed to ensure that the ability to cast an informal vote remains possible, so as not to curb political speech.

53 See, for example, Asahi Simbun, *Electronic Poll Goes Smoothly* (25 June 2002) Japan Today <http://www.japantoday.com/e/tools/print.asp?content=news&id=220262> at 29 June 2002 (counting the ballots in a recent Japanese trial took three hours shorter than the previous, similar elections).

54 Department of the Parliamentary Library, above n 36, 1.

tribution of preferences than the traditional voting methods.[55] As post-election counting can stretch for long periods in Senate elections, any system that hastens the counting process would be welcome.

Moreover, a properly maintained e-voting system is unquestionably accurate, thereby reducing the instances of losing candidates questioning the count, requesting a recount, or otherwise lengthening the process in close elections. Another connected benefit of e-voting is the elimination of human error or prejudice. While human error occurs in every election, rarely does it ever accumulate to the point of deciding an election. In the 2000 Presidential election, however, a combination of human error, poor electoral structure and other faults combined to send the Florida election into disarray.

Moreover, as the media increasingly uses technology and opinion polls to predict election outcomes before their conclusion, the importance of quick election results has never been so crucial. But, short of a ban on such 'speech', the electoral system risks being compromised if it cannot quickly tally the vote. By allowing the media the opportunity to announce election results (regardless of their accuracy), the Australian Election Commission ('AEC') risks diminishing the significance of the Western Australian vote, as voters there may feel their vote is unimportant if the parliamentary result is already a certainty. The AEC cannot ignore this reality and must actively attempt to eliminate this growing problem. Internet voting, with its quick tallying ability, should be studied as a potential solution.

Long-Term Savings

The cost of administering an election under the current system is substantial,[56] and while the short-term costs of implementing any form of Internet voting will be considerable, e-voting has the ability to lower significantly the cost of elections in the long-term. For instance, Internet voting at the polling station would ease the administrative and financial burden election officials currently face in securely monitoring, storing and transporting ballots. In addition, as less paper would be printed for ballots, e-voting would save the monetary and environmental cost of printing ballots. Jurisdictions al-

[55] Ibid.

[56] The 2001 federal election cost $107.8 million, $68 million of which was paid to the AEC: Louise Dodson, 'Price of the vote tops $100m', *The Age* (Melbourne), 5 December 2001, 1.

ready using e-voting concur with this assessment and report substantial savings since abandoning traditional voting.[57]

Remote Internet voting could potentially save electoral commissions even more money, as remote voting removes the need to maintain as many polling stations on election day, thus reducing the number of polling staff and training costs for the electoral commission. In addition, remote voting would substantially reduce the amount spent on the voting infrastructure, and would also reduce the number of printed materials and ballot papers.

Start-up costs appear to be a major stumbling block to any form of online e-voting, and may be prohibitive to implementing an e-voting system. Once the initial outlays are out of the equation, however, e-voting offers substantial savings over the present system of voting. Studies must be conducted to calculate the long-term costs of an e-voting system to ascertain if the system is cost-effective to implement.

Higher Voter Turnout

Voting is at an all-time low in many nations without compulsory voting.[58] Although this article focuses on Australia, where voting is compulsory, it is worth mentioning that voter participation is a key reason that some nations have initiated studies on Internet voting.

Two nations particularly concerned with voter participation are the United States and Britain, where citizens under the age of 40 seem disenfranchised from the democratic process. Both nations have instituted reforms to increase participation with little effect on the electorate.[59] Both nations have indicated a willingness to invest in and trial remote Internet voting as a possible cure to this modern day

57 See Kevin Coleman, *Internet Voting: Issues and Legislation*, Congressional Research Service Report for Congress, 7 November 2001, 2.

58 Britain managed only a 59 per cent turnout for the last general election, thought to be at its lowest point since universal suffrage was introduced. See Jackie Ashley, 'Sir Robin Cook, Leader of the House of Commons, Plans to Make UK First to Vote on Internet', *The Guardian* (London), 7 January 2002 <http://politics.guardian.co.uk/commons/story/0,9061,628777,00.html> at 15 January 2003. In the United States, just over half the eligible voters voted in the 2000 Presidential election, compared with 63 per cent in the 1963 election: *Report Pans Internet Voting* (6 March 2001) Wired News <http://www.wired.com/news/print/0,1294,42229,00.html> at 29 May 2002.

59 Reforms have taken the shape of numerous options, such as simpler registration procedures, liberalising the absentee and postal ballot requirements, and extending voting times.

lethargy.[60] It is hoped the convenience of online voting provides the extra incentive to encourage greater participation at the polls.[61]

While the cause of voter apathy is debated, it seems clear that Internet voting has the ability to increase voter participation. Several trials conducted over the Internet, including the 2000 Arizona Democratic primary, substantiate this claim. In fact, the Arizona Democratic primary saw voter participation rise 600 per cent over the last election, with 41 per cent of the 86 907 votes cast via the Internet.[62]

Experience/Analysis in Internet Voting

The United States

In the United States, a number of e-voting trials have taken place recently, including the Arizona Democratic Party primary, a trial operated by the United States Department of Defense, and several non-binding trials run by private software companies.

Arizona Democratic Party Primary

Of the American trials, the Arizona Democratic primary garnered the most considerable media attention.[63] The trial, trumpeted as 'the first-ever, legally-binding public election over the Internet',[64] succeeded in increasing voter interest. Although the Arizona Democrats and the system designers, Election.com, declared the trial a success, the trial came under criticism from outside observers for numerous reasons.[65]

60 In Britain, Robin Cook strongly supports remote Internet voting for the next general election as a way to 'enfranchise' those back into the democratic process. See Ashley, above n 58.

61 The fear is that Internet voting may only be a short-term solution to voter apathy and that its implementation will actually depress participation in the long run as it could be perceived as undermining civic participation and the legitimacy of the act of voting: Internet Policy Institute, above n 8, 25.

62 Arizona Democrats, *Paper Ballots v Internet Votes* <http://azdem.org/breakdown.html> at 26 May 2002. It is important to note that total voter participation in the election still totalled fewer than 10 per cent of registered Democrats: ibid 24.

63 Internet voters in the Arizona Democratic primary, an internal party election governed by the rules of the party as opposed to under the scrutiny of election officials, voluntarily chose to cast their ballot online.

64 John O'Looney, *Implications of Internet Voting* (2000) Government Technology <http://www.govtech.net/magazine/gt/2000/sept/Internet/implications/html> at 19 May 2002.

65 The election only went forward after a court refused to grant an injunction filed by the Voting Integrity Project ('VIP') to stop the election. The VIP argued that

While this landmark trial should be commended for being the first major election to use the Internet and for putting e-voting issues on the agenda, the trial did have substantial shortcomings that need to be addressed. First, the election lacked the safeguards normally present in a democratic election. Namely, the company hired to oversee the election operated the trial without the supervision or certification of trained election officials. Election officials are trained to maintain standards and would have increased the reliability, integrity and image of the trial. Moreover, Election.com and the Arizona Democrats failed to record statistically the amount of voters who attempted but failed to cast their vote over the Internet. Such statistics would be relevant in analysing the success of the trial.

Second, the system used in the election lacked adequate security and verification procedures. Voters were mailed a personal identification number which the voter used, in connection with other easily obtainable personal information, to activate the e-voting system. Many potential Internet voters, however, failed to receive their PIN number and were forced to travel to the polling station to vote. Moreover, Election.com did not provide for a sophisticated enough tracking system to ensure that the proper person was voting, thereby increasing the possibility of fraud during the election.

In addition, the election did not provide adequate safeguards against the possibility of an online service denial. Thus, if too many voters attempted to vote at the same time, or if a hacker flooded the system, a service denial would have ensued, thereby disenfranchising voters who may not have another opportunity to vote. Moreover, numerous potential Internet voters could not participate in the trial due to the incompatibility of their computers or web browsers.

Even with the problems and concerns created by the administration and management of the election, the Arizona Democrats deserve credit for starting the Internet voting revolution. This trial created

the election denied equal access and discriminated against certain voters because Internet voting would last four days instead of the usual one day period, and drew attention to a recent Department of Commerce report showing white people were more likely to have home Internet service than racial minorities (thereby increasing the number of white voters as the number of minority voters remains or increases at a lower rate). The judge suggested that the election would not stand if racial discrimination resulted and the Justice Department announced it would review the election results. Interestingly, the VIP's argument is counter to their paper entitled, 'Are We Ready for Internet Voting', which argues voter convenience would lower participation among Internet users, thereby serving not to lower minorities' voting power but actually increasing the power. See ibid.

media and political attention to the issue and paved the way for other trials to build upon the knowledge gained in this trial.

Department of Defense

The United States Department of Defense Federal Voting Assistance Program developed and trialled an Internet voting system for military personnel located outside the United States.[66] While the trial took some years to develop and the cost incurred proved considerable, the end result was a successful trial at the 2000 United States Presidential election.

The Defense Department contracted with a private company to develop and implement the entire technical environment for the trial. The finalised system consisted of a customised computer application capable of handling the voting process. In order to cast their ballot, voters logged on to the designated website and entered their security PIN, which had been provided for the trial. This process of logging in activated the security (PKI technology).[67] Once securely logged on to the site, voters selected their preferred candidates and completed the voting process. After voting was completed, local voting officials in every applicable county logged on to the site and entered their previously distributed PIN to retrieve the votes.[68]

The trial proved costly for a number of reasons. First, the Defense Department had to fund the development of an e-voting system without having a model on which to construct their system. Second, the Defense Department had to organise and train participants and state and local election officials for the trial. In this regard, support from individual states was crucial, as each of the four states involved amended its legislation to allow the 250 triallist to cast their ballots

66 The Federal Voting Assistance Program, the agency that administered the trial, issued a report evaluating the trial, available at <http://www.fvap.ncr.gov/voi.html>.

67 Digital signature authentication appears to be the best way of protecting voter privacy and secrecy. However, the cost of the technology could be prohibitively expensive to most jurisdictions: David Elliott, *Examining Internet Voting in Washington*, State of Washington White Paper (2001) 4 <http://www.electioncenter.org/voting/InetVotingWhitePaper.html> at 3 May 2002. Moreover, claims have been made that use of a cryptography key ('PKI') is not proven effective against hackers or other faults over the Internet: Barry et al, above n 6, 14.

68 Officials decided that allowing the system to tally the votes would have been too big a step to introduce in the trial. Therefore, the trial focused on the system and security aspects of e-voting. Election officials printed out a non-identifying ballot for each voter for the purposes of tallying votes.

over the Internet.[69] Third, the Defense Department provided each voter and official with an individualised PIN and also provided each voter with a CD-ROM to guarantee that the voter's web browser had adequate security and technical compatibility capabilities. In a larger electorate, sending PIN numbers and CD-ROM browser updates to every potential voter would simply not be secure or economical. Even in this trial, there were instances of voters losing their PIN numbers and even of people attempting to vote using their partner's PIN.

The Department of Defense trial produced positive results for e-voting and should be considered an advancement for Internet voting. The limited scope of the trial, as well as the safeguard methods used, provided for a secure and successful e-voting election. However, the applications used and security safeguards developed in the trial, such as sending a PIN number and CD-ROM to every voter, cannot be safely and economically implemented on a widespread basis.[70]

Non-Binding Trials

Non-binding public and binding private elections are increasingly common and have generally been successful.[71] As companies are increasingly allowing shareholders to vote via the Internet on a wide range of topics, several private companies have been given an opportunity to showcase their Internet voting software. Australia has even taken part in these private elections, with NRMA shareholders voting for the board of directors online in 2001.[72]

The most notable private e-voting software companies include VoteHere.net,[73] Election.com,[74] and Safevote.com. Voters seem to

69 Voters were covered by the *Uniformed and Overseas Citizens Absentee Voting Act*, 42 USC § 1973ff. Eligible voters must have had legal residence in one of the counties allowed to participate in the trial (each state was limited to only one county participating in the trial as a security measure to limit risk exposure in the event of system failure).

70 Moreover, the process of receiving and installing the CD-ROM as well as guarding a PIN number may dissuade people from participating in the process.

71 See Dictson and Ray, above n 34.

72 See *NRMA Selects election.com to Conduct One of the Largest Private Sector Elections in Australia* (2001) Election.com <http://www.election.com/au/0130.htm> at 15 January 2003.

73 VoteHere.net conducted a trial in the state of Washington at the 1996 Presidential election. The trial aimed to introduce the concept of e-voting to the electorate. After voting in the binding election, voters could elect to cast their non-binding vote at an Internet voting station. The e-voting system was well received by the majority of those who participated. The trial received considerable media attention and may have started the quest for e-voting in the United States.

approve of the system used for voting, as well as the ease and convenience Internet voting offers, and there have not been any major security breaches for elections of this nature. Whilst public elections attract more publicity and passion and have to comply with more rigorous standards, private elections conducted over the Internet contribute to the development of better voting software by allowing companies to assess and correct performance after each vote and are a useful platform for election officials to trial e-voting software.

In November 2000, Safevote.com conducted one of the most comprehensive and successful mock elections. Safevote.com invited voters who cast their pre-poll vote in Contra Costa County, California to cast a mock vote via the Internet. Participating voters were given a PIN to activate the system and used a mouse to select their preferred candidates.[75] Once a voter completed the process, their vote was stored on a completely separate system to prevent the voter's identity being traced to their vote.[76]

In addition, Safevote.com encouraged people to hack into the system and even published the hardware and software details on the Internet, hosted an attack help page, and created an attack hotline to encourage hackers to attempt to crack the security. The system remained secure throughout voting. Safevote.com attributes their record of security to its use of a constantly changing IP address used to connect the system to the Internet. The revolving IP address makes flooding the system and hacking difficult, if not impossible. Just as encouraging, 100 per cent of the 300 people who voted using the system found it easy to use and understand, including an 80 year old woman who had never used a computer, and a drunken man, who stated, 'If I can do this, anyone can.'[77]

74 Election.com managed the election for the Arizona Democrats, the board of directors of Internet Cooperation for Signed Names and Numbers ('ICANN'), and for the Australian NRMA board of directors.

75 The PIN numbers were calculated using a voter's date of birth and the type of ballot requested. The voter verification system checked the PIN against the database and enabled the voter to verify their vote before submitting it for tally.

76 This security and privacy measure is common among all the major e-voting software companies.

77 See Farhad Manjoo, *Ballots Need an Upgrade – Duh!* (10 November 2000) Wired News <http://www.wired.com/news/politics/0,1283,40078,00.html> at 15 January 2003.

The United Kingdom

In May 2002, the British government provided £3.5 million to undertake a series of initiatives aimed at improving electoral efficiency, encouraging voter participation, and widening the range of voting methods. Election officials tested a range of innovations in 30 local electoral districts.[78] The trials allowed electorates to conduct voting via the Internet, text messaging or offline e-voting at the polling station.[79]

Prior fears of security breaches and increased electoral fraud appeared unfounded, as the system functioned properly and there were no technical glitches or known security breaches.[80] In addition, e-voting facilitated accuracy and efficiency in tabulating the ballots. Perhaps the most shocking result of the trial was the fact that e-voting did little to improve participation,[81] with participation rising only 5 per cent in areas with e-voting at the polling station and a paltry 1 per cent with remote Internet voting.[82] The main reason for the turnout is the lack of importance given to local elections by most voters. Significantly, however, those who used e-voting methods were positive about the experience and found them easy to use. In fact, 45 per cent

78 The *Representation of the People Act 2000* (UK) provides for local councils to apply to run pilot schemes. Over 40 local authorities applied, with over half involving some form of electronic voting. See Electoral Commission, *Modernising Elections* <http://www.electoralcommission.gov.uk/about-us/modernisingelections.cfm> at 9 January 2003.

79 The United Kingdom trial allowed voters to vote up to a week before election day via mobile touch screen electronic voting machines (offline), via the Internet, and even by telephone or text messaging: *Britain Experiments with Early, High-Tech Voting* (25 April 2002) AP World Politics <http://www.story.news.yahoo.com/news?tmpl=STORY&U=/ap/200204.../britain_high_tech_voting.htm> at 9 June 2002.

80 See *Online Voting Fraud Warning* (5 February 2002) BBC News <http://www.news.bbc.co.uk/hi/English/uk_politics/newsid_1799000/1799883.stm> at 9 June 2002; Wendy Brewer, *E-Voting Has a Long Way to Go: Election Results Mixed for Alternative Voting Methods* (3 May 2002) PC Advisor <http://www.pcadvisor.co.uk/index.cfm?go=news.view&news=2266> at 28 June 2002.

81 Overall, turnout for the elections was higher than recent elections, with participation varying widely among pilot districts (with some districts matching polling figures of the 2001 general election, while others showing little or no increase). See Electoral Commission, above n 78.

82 Brewer, above n 80. NOP data indicates 23 per cent of the voters in districts with e-voting were aware of the methods of voting and were encouraged to vote because of them (with 72 per cent saying the new technologies made no difference in encouragement). Seventeen per cent of non-voters said the new technologies gave them encouragement to vote, yet they still did not vote. See ibid.

of those polled thought that e-voting made the process of voting 'better'.[83]

While e-voting did not have the increase in participation officials had hoped for, the system proved itself secure and voters approved of the voting technologies. Therefore, the primary aim of the trial, to establish the reliability and security of the e-voting systems and to build public confidence in the new technologies, achieved its objectives.

Legislative Security

A system of e-voting built on a weak legislative foundation could possibility create the opportunity for electoral challenges and lawsuits. The absence of tangible public scrutiny and a recognisable audit trail could potentially trouble losing candidates and their supporters, and may also lead to challenges in the courts.[84]

While legislation cannot avoid such questions, legislation can and must be drafted in such a way as to minimise these instances from occurring. The prospect of implementing any form of e-voting requires substantial review and reform of the current electoral laws. The current system effectively handles conventional voting offences and abuses but may not be sufficient for new risks e-voting may pose. In order to implement any form of e-voting, the various Commonwealth and State electoral Acts would have to be scrutinised to ascertain which sections would need amending to accommodate the technology. For instance, the Act refers to 'ballot-papers' and makes numerous other references to traditional forms of voting, all of which would have to be amended.[85] In addition, provisions relating to a 'recount' and events which trigger such an action would also have to be amended and updated for e-voting. Moreover, it would be imperative to add several new sections to the Act regarding the tabulation of the votes, such as an amendment banning election officials from releasing voting information until the close of the polls around Australia (as the

[83] A similar proportion claimed the new technologies made no difference.

[84] This argument against computerised voting is rarely valid and candidates often quickly abandon such allegations and move onto electoral administration or other reasons to blame for their loss. For numerous instances of this occurring in the United States, see <electionline.org> at 15 January 2003.

[85] Other issues that need revisiting are provisions governing the recount, ballot secrecy, and privacy issues.

publication of results before other stations have closed could dissuade voters from voting).[86]

In addition, special care would need to be taken in drafting provisions relating to the criminalisation of all forms of corrupting or tampering with, or attempting to corrupt or tamper with, polling station e-voting machines. While some provisions of various electoral Acts contain blanket statements against interfering with the electoral process, the accuracy of the machines is essential to the success of an election under e-voting, therefore special consideration in the Act and stiff penalties would have to be specifically addressed.

While the amendments needed to implement e-voting stations at polling booths appear straight forward, amending the Act to allow remote Internet voting is a more complicated task. For instance, if the election were conducted over the Internet, the Act would have to be further amended to prohibit and criminalise a person from stealing, coercing, buying, selling, or giving away their digital signature and/or vote.[87] In addition, the Act, in association with other laws, would have to criminalise all forms of hacking into the voting system, as well as jamming or reducing access/spamming the voting system to prevent the officials from responding to legitimate requests.[88]

Moreover, amendments must also prohibit persons from page jacking or spoofing sites for the purposes of intentionally deceiving or otherwise impeding the legitimate user in casting their vote. Further, the legislation should also include a section criminalising the invasion of privacy by attacking a ballot or website with intent to examine or change votes. Election officials may also want the Act amended to prohibit private companies and political parties from conducting onscreen advertising during the voting period. While most onscreen advertising would be harmless, the potential for advertisements to deceive or lead voters away from the authorised site could produce a confused electorate.

Another primary concern associated with Internet voting is one of jurisdiction. As the Internet is not controlled by one sovereign entity, instead being an uncontrolled, international medium, the government

86 Prohibiting officials from even collating the results may be considered to prevent leaks to the press.

87 While anti-bribery laws may arguably already cover such activities, specifically legislating against such activity is recommended.

88 Again, while the Act has provisions banning the intentional interference with electoral administration, specific sections criminalising this activity is recommended.

and election officials need to consider seriously the consequences of implementing remote Internet voting. The law relating to a security breach or act of fraud occurring online due to the conduct of a foreign national not in the jurisdiction is an unsolved problem. Leaving aside the issues of even finding the culprit, an overseas, foreign national may not be subject to prosecution within Australia without the use of long-arm statutes and extradition treaties.[89] As foreign laws may differ in their criteria for an offence or in their application, the foreign nation holding jurisdiction over the offender may not submit the offender for extradition.

The Future

Gradual Introduction

Internet voting trials have been successful and encouraging, yet e-voting software companies are nowhere near providing a cost effective, remote e-voting system that can guarantee the level of security, authentication, privacy and accuracy that democratic elections command. For this reason, a slow, evolutionary change is needed to introduce e-voting into our electoral culture.[90] Such change can be accomplished through a gradual introduction of e-voting, achieved by a two-phase introduction approach. Phase 1 would utilise Internet voting technology in the existing polling stations by allowing voters the choice of voting at the polling station via the Internet or by traditional methods.[91] Phase 2 would eventually introduce remote Internet voting to the electorate when the technology is ready and when the

[89] The use of reciprocal agreements to effect multinational jurisdiction and enforcement actions, such as apprehension and extradition of suspects, is crucial to successfully implementing remote Internet voting. Failing this, nations will have to rely on international laws to respect the democratic elections and processes of a sovereign nation and protect that nation from incursions that seek to undermine the security and stability of a nation's democratic process. For more analysis of issues surrounding international criminal action, see Louis Henkin et al, *International Law: Cases and Materials* (1980) ch 7; I A Shearer, 'Extradition and Asylum' in K W Ryan (ed), *International Law in Australia* (1984) 179-201.

[90] See, eg, California Secretary of State, above n 27; Barry et al, above n 6; Hoffman, above n 33.

[91] While acknowledging the long-term benefits of remote Internet voting, the Internet Policy Institute report instead recommended Internet voting at the polling station, where election officials could maintain control of the security and technology. The report reiterated the point that e-voting systems require a much greater level of security than e-commerce, a level of security that remote Internet voting 'will not be able to meet ... for years to come': *Report Pans Internet Voting*, above n 58.

voters have sufficient confidence in e-voting systems. This slow, gradual approach would allow for constant monitoring, security, testing and improvements, and would avoid introducing a radical change that could potentially weaken voter confidence in the electoral process.[92]

In order to become part of the electoral process, Internet voting needs to be further funded and studied across a wide range of disciplines. Specifically, technical experts need to study and improve the e-voting systems overall, including security and encryption technology, so that election officials can safely implement the system to the widespread voting public.[93] In addition, political scientists must study the effect of Internet voting on public confidence in the electoral process, the effect on participation, and the effect on the character of elections. Finally, lawyers need to analyse the existing electoral laws and develop new laws which ensure that electoral failure does not result from a legal breakdown.

The most crucial aspect to the eventual implementation of an Internet-based e-voting system is the voting trials.[94] Only with experience can election officials really gauge how a system works, and only with experience can technical experts, social scientists and lawyers assess the strengths and weaknesses of a system and make it a viable option for elections in the future. Controlled trialling of polling station and remote Internet voting with overseas voters would prove useful. The potential barrier to implementing a trial of this magnitude would be the substantial amount of planning and resources required to successfully implement such a system.

92 See California Secretary of State, above n 27, 2.

93 Electoral officials would be wise to consider a certification programme for any e-voting system. The programme should have strict security and reliability standards as well as strong verification of systems. It would also be wise to use pre-existing open source code e-voting systems as models to base improvements upon. While the use of open source codes may inhibit some intellectual property rights, the trade-off of a more secure system that is open to public scrutiny far outweighs the negative effect on proprietary rights.

94 The Internet Policy Institute report states that trials could be used 'to gain valuable experience prior to full-scale implementation': Internet Policy Institute, above n 8, 2. 'The security problems that might arise might well undermine the legitimacy of the electoral process' said David Cheney of the Internet Policy Institute. 'We must dispel the myths associated with Internet voting and educate public officials to avoid this scenario': National Science Foundation, 'Internet Voting is No "Magic Ballot": Distinguished Committee Report' (Press Release, 2001) <http://www.nsf.gov/od/lpa/news/press/01/pr0118.htm> at 15 January 2003.

Potential Australian Trials

A number of markets exist within Australia for limited scale Internet voting trials. While these trials would not be risk-free, they should initially be limited enough in their scope to not call an election result into question.

Limited Pre-Poll and Polling Station Voting

The first step towards an online, e-voting option could be at the polling station for a limited number of voters. This limited trial could take place at select pre-poll locations or even select polling stations on election day to test the security, accuracy and ability of the e-voting system, as well as to provide the voter more convenience and voting options.[95]

The trial would also introduce the concept of Internet voting to Australians in a comfortable atmosphere without radically changing the familiar voting surroundings. Over time, and with successive successful elections with Internet voting, hopefully citizens will get acclimated to the system and acquire the same level of confidence in Internet voting that they have in traditional voting methods.

Australian Antarctic Electors

The first voters to trial remote Internet voting could be the Australian Antarctic electors. Similar to the United States Department of Defense trial, voters could be given a PIN and vote via secure Internet connection. As the number of Antarctic voters is very small, the risk of fraud or impersonation is very low. However, the small number of voters also calls into question the privacy of each voter's identity.

While this initial trial may be too limited and small scale to provide any substantial data, it would be a good opportunity to test the security and accuracy of the system, as well as the structure of remote Internet voting. Moreover, the significant media coverage this trial would likely attract would aid in the process of funding and further expanding the trials.

[95] As no online trial has been attempted in Australia, the trial would be similar to the United States Department of Defense trial, and limited in size and scope to only involve a certain percentage of the electorate, which, in the unlikely event of failure, would not have a great impact on the election results.

Overseas Voters

Another trial of Internet voting could be implemented for overseas voters. This option could be implemented in a number of different ways and could be used to trial polling station or remote Internet voting. In addition, as there were 65 000 overseas voters at the 1998 federal election and 5000 overseas voters in the 1999 Victorian State election, the trial would have a sizeable number of participants and yield a substantial result.[96]

One possible trial could simulate polling station voting and have overseas voters being given the option of voting via the Internet at the selected overseas polling station (possible locations include the local Australian embassy or diplomatic mission).[97] Voters would attend the designated polling station, and, after clearing the normal identity checks, cast their vote electronically via the Internet. Once polling has ended, the secure polling station server could send the votes via the Internet to secure servers in the appropriate jurisdiction of each voter.

Another, more advanced option for an Internet trial would allow voters the opportunity to register as an overseas voter and be given the option of voting remotely over the Internet. In the initial stages, voters would likely be given PIN and CD-ROM (for reasons of security and browser compatibility), but with time, other, less intrusive methods could be trialled. Voters would then log on to the voting website from any location and cast their ballot via the Internet.

Another alternative for trialling Internet voting with overseas voters would simply update the current process used for postal voting, whereby requested ballots would be distributed via secure email. The voter would then have the choice of returning the ballot via secure e-mail or printing out the ballot and returning it, along with their signature for verification, via the post. This system has numerous benefits to the voter and the electoral process, as the system would substantially cut-down the bulk and costs of election materials sent overseas during the election campaign, and the process would not be a radical departure from the traditional postal vote.[98]

96 Barry et al, above n 6, 17.

97 Polling stations could either have hard copies of the electoral roll or access the roll electronically to verify the voter is eligible to vote and in which jurisdiction.

98 The limited scope of e-voting would also eliminate any fears of web server transmission bottlenecks during peak voting periods.

Conclusion

After the initial euphoria surrounding the prospects of Internet voting swept the electoral world, the issue was studied in further detail and the promise of Internet voting convenience was replaced by overarching issues of security and reliability. But the public's yearning for 'all things Internet' continues, and pressure to implement some form of Internet voting will only mount.[99] Already, a few European countries have implemented Internet voting,[100] with numerous other European countries either trialling or announcing their intention to trial and implement Internet voting.[101] In addition, the United States has announced it will expand Internet trials in the 2004 general election.[102] When the pressure grows in Australia, election officials and politicians need to be armed with research and information so they can make informed, responsible decisions regarding the future of Australian democracy.[103]

99 See Eileen McGann, 'Is Internet Voting Fair?', *Network World*, 26 June 2000, 61; 'Voters Overwhelmingly Support Internet Voting', *Business Wire*, 1 March 2000 (reporting a poll conducted by Votehere.com indicated 94 per cent of the 3638 polled indicated a desire to have Internet voting offered as a voting option in the future).

100 Estonia plans to have online voting in the 2003 elections and the Swiss canton of Geneva plans to allow remote Internet voting in 2003 local elections: Dermot McGrath, *Europeans Eye E-Vote Eventuality* (22 April 2002) Wired News <http://www.wirednews.com> at 2 May 2002; Alison Langley, 'Geneva Suburb Casts Ballots on the Internet in Test Project', *New York Times*, 12 January 2003 <http://www.nytimes.com/2003/01/12/international/europe/12SWIS.html> at 15 January 2003.

101 Britain announced its intentions to expand its Internet trials in 2003. See Office of the Deputy Prime Minister, 'May 2003 Elections to Continue Online Voting Trials' (Press Release, 27 September 2002)
<http://www.odpm.gov.uk/news/0209/0086.htm> at 15 January 2003. Germany announced it will have online voting by 2006, and France, Italy and Spain have planned e-voting experiments in forthcoming referenda and elections: McGann, above n 99. A number of these initiatives were funded by the European Union. See Cybervote Project, 'Vote in Total Confidence Via the Internet' (Press Release) <http://www.eucybervote.org/press_release.html> at 15 January 2003.

102 The Federal Voting Assistance Program is developing a system called the 'Secure Electronic Registration and Voting Experiment' for the 2004 elections that will provide Internet registration and voting to overseas citizens. At present, 14 states are participating in the project. See Digital Government Program, *Military Voting Goes Online*
<http://www.diggov.org/news/stories/2002/0402/0402military_holland.jsp> at 15 January 2003.

103 Because issues relate to security, convenience and cost, the research must be cross-disciplinary and include social scientists, IT specialists, electoral administrators and lawyers in a collaborative effort.

Remote Internet voting has numerous technical and social science issues that require attention before it could become a safe and reliable alternative to traditional voting methods. Remote Internet voting may also pose significant risks to the integrity of the process.[104] As many of the problems threatening to plague remote Internet voting cannot presently be resolved without substantial burdens to the voter, the prospect of remote Internet voting appears to be a long-term hope rather than a short-term goal.

The United States Presidential election of 2000 proved that the current voting systems regularly used today are not infallible.[105] Equipment once thought of as near perfect electoral aids, such as the lever-operated machines and punch card readers, in fact could, and have, become highly contentious and undesirable in many settings. Moreover, electoral problems such as fraud, deceit, bribery, abuse, ballot tampering and multiple voting are frequently part of every election in some form. While this is not a significant problem in Australia, all of the above have occurred,[106] and, at the very least, it proves the cur-

[104] While many commentators feel Internet voting is safe at the polling station, some do not believe the electoral process is significantly developed enough for remote Internet voting. See, for example, James Nevin Jr, 'Obstacles to Internet Voting: Perceived Problems with Security and "Digital Divide" Vote Dilution' (2002) 6 *West Virginia Journal of Law and Technology* 2.1. These commentators believe the risk of someone hacking into a voter's personal computer and altering the vote before the encryption device begins to operate is real and substantial. Compare Internet voting at the polling station, where election officials control the PCs and the risk of hacker attacks is virtually, if not completely, eliminated.

[105] Ironically, the failing of traditional voting methods in Florida stunted the progress of technological advancement. Instead of moving forward with major initiatives, post-Florida electoral officials are concentrating on fixing the present system before embracing an alternative voting system. Ed Gerck, CEO of Safevote.com, stated, 'I would say Internet voting would have been better served without Florida. The same way Florida advanced the need for technology, [was] the same way Florida highlighted the tremendous risks': Farhad Manjoo, *Net Voting? Keep Your Pants On* (7 February 2001) Wired News <http://www.wired.com/news/politics> at 9 May 2002.

[106] See, for example, Peter Grabosky, *Wayward Governance: Illegality and its Control in the Public Sector* (1989); P Finn, 'Electoral Corruption and Malpractice' (1977) 8 *Federal Law Review* 194-230; Amy McGrath, *The Frauding of Votes* (2001). There have been prosecutions and imprisonments for violating the Australian *Electoral Act*. For example, recently in Queensland three people were convicted of fraud relating to their participation in the registration of Australian Labor Party members for pre-selection seats. The convictions led to three commissions: the Queensland Criminal Justice Commission (2001) (now the Queensland Crime and Misconduct Commission), the Queensland Legislative Assembly's Legal, Constitutional and Administrative Review Committee (2000) and the Commonwealth Parliament's Standing Committee on Electoral Matters (2000).

rent system is not perfect. Therefore, the system should be able to grow and adapt to technological development and change.

In the long-term, the question becomes to what level of risk should Internet voting be judged? Should Internet voting be held to the same standard of traditional voting or to a higher standard? Most problems associated with Internet voting are not foreign to the electoral process, just problems cast in a different form. Security and other weaknesses are inherent in the traditional voting methods, so to hold e-voting to a 100 per cent secure record would be unfair and create a different playing field. While remote Internet voting for the general population may be some time off, its long-term promise could be tested in trials involving Australian Antarctic electors or even overseas voters.

In the short-term, Internet voting at the polling station could feasibly be instituted within the next few election cycles. The moderate benefits of Internet voting at the polling station, such as less informal votes and quick, accurate results, come with considerably less risks than remote Internet voting. In addition, as voters would still go to the polling station on election day, Internet voting at the polling station has the added benefit of involving less political culture issues.

Internet trials and further study into the area are needed to assess the viability and risks of Internet voting in Australia. Therefore, it is imperative that election officials have the foresight and initiative to actively research this important area of our democracy. Further, and maybe of equal importance, Internet voting can only be implemented when the level of risk associated with its implementation is acceptable to election officials, politicians and Australian voters. While it appears that currently, Internet voting at the polling station is a reasonable level of risk, the level of risk presently associated with remote Internet voting is simply too great. Maybe, in time, the information garnered from further trials and evolutionary introduction of Internet voting will cause election officials and the voting public to accept remote Internet voting as a safe, effective and efficient way to vote.

The committees all concluded that the cases of enrolment fraud could not have affected the results of any federal, State or local election.