Still Under Construction: Voting And The Internet Superhighway

Many voters seek the convenience of voting over the net. Bryan Mercurio examines the technical difficulties of e-voting and its possible impact on voting culture.

The accessibility, relatively low cost, and seemingly endless capabilities of the internet have expanded the medium beyond our recent imagination. Perhaps in response to the media-driven euphoria surrounding its capabilities, users of all ages, and particularly the younger generation, increasingly demand more from the internet. Users have created an internet "bandwagon" which continues to show enthusiasm for "all things internet". Voting "customers" have leapt on the "bandwagon" and increasingly demand more convenience within the electoral system with the use of technology.

Some commentators believe that remote internet voting is the future of voting as it would use technology to add needed convenience to the electoral system. Proponents of remote internet voting envision voters logging onto the voting website via secure means, establishing their identity, and then voting in a real-time transaction. This simple to understand formula is similar to any other web-based transaction and would allow voting at the voter's home, the office, café, or anywhere else the voter can access the internet.

While we are still some time off securely implementing remote internet voting in a federal election, the public's increasing reliance on the internet for personal and business communication leads many to conclude that internet voting is inevitable. While enhancing voter convenience in the electoral process is a goal worth achieving, it cannot come at the expense of fundamental electoral values such as cost, reliability, accuracy and security. While there are numerous potential problems with internet voting, this article analyses five key concerns relating to remote internet voting of which the public should be aware.

Voting is unlike any other online transaction

While private companies accept there will be a degree of fraud in their online transactions, the electoral process does not have the same luxury. The election of our parliamentarians is a symbol of our democracy and maintaining the integrity and accuracy of the process is essential to preserving a thriving democracy. If citizens lose confidence in the electoral process, the nation loses its credibility, honour and, ultimately, its democracy.

The proper authentication of votes is a necessary criterion for a successful election. Elections must ensure that only eligible voters cast ballots on election day and that those voters cast their own ballot and do so only once in the election.

The problem for internet voting is authenticating votes without losing the benefits of the extra convenience for the voter. Commentators have suggested numerous different formats regarding the implementation of a successful remote internet voting regime that properly authenticates. One method would require the voter to encrypt the ballot with a secret key before sending it to the electoral office. 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 his/her 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 e-voters for those voters to verify that their names are listed and 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 the voter would sign and return. 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 the above examples would provide voters the chance to cast their ballot via the internet from anywhere in the world. Both examples also attempt to provide security by adding layers of protection-related actions required by the voter, thus limiting the benefits of e-voting convenience and adding to the cost of administering the election.

The unanswered question is whether these methods will provide adequate security against vote selling, vote swapping and voter fraud. If not, do we as citizens want to subject ourselves to biometric scanning procedures, such as retinal or finger-print scans, just to get the added convenience of voting away from the polling place? Such measures seem intrusive and probably unacceptable to most voters. Therefore, the price of a secure election may outweigh the benefits of added convenience and may be too high for some voters to accept.

Moreover, private companies can send an order confirmation to the customer as a receipt of the transaction. That is a luxury which the electoral process does not have, as our elections must maintain the secrecy of the voter's ballot. An online system of voting must ensure it can authenticate an online ballot while at the same time preserving the voter's right to cast their ballot in secret. This is just one of many unique aspects to internet voting which must be considered before its implementation.

Remote internet voting is susceptible to fraud

While some form of fraud could be present in any election, regardless of how voters cast their ballot, remote internet voting is particularly susceptible to fraud due to the inherent problems with security over the internet. Online security breaches can occur in two ways:

- by an attack which targets the client or server directly (commonly called a penetration attack); or
- by an attack that targets and interrupts communication between the client and the server (commonly called denial of service).

Penetration Attacks

Penetration attacks occur when a hacker delivers a virus to a target computer, usually transported by floppy disk, CD-ROM, e-mail, or by exploitation of an existing bug or security flaw in the target's computer or browser. Attacks such as these are quite common and difficult, if not impossible, to defend against. Once the hacker has the virus in place, they can do as they please and can easily spy on users casting their ballots, prevent users from casting their ballots, or even modify a voter's ballot. 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. Therefore, 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 and result of the election.

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 process could include having the internet voter pre-register to vote online, sending the voter a CD-ROM to install prior to voting, and sending a password and PIN number to the voter.

Denial of Service Attacks

Denial of service attacks focus on the path between the computer user and server. In effect, the hacker attempts to overload a website with requests for information, thus "jamming" the lines and preventing others from using the site. Currently there is no way to stop the "jamming" without shutting down the system and thus shutting out legitimate users for the site until the problem is diagnosed and resolved. Therefore, before implementing remote internet voting, election officials must ensure that the transmission between voters and its server is authenticated and encrypted so that hackers cannot corrupt

the vote process whilst the transmission is en route. Current technologies can ensure the latter, through encryption technology such as public key infrastructure. Maintaining the authenticated communication link between user and server cannot presently be guaranteed.

A successful remote internet voting system must also protect against a plethora of other hacker activities. One is "man in the middle", which 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. Another is "page jacking", which involves a hacker leading a user off the intended website and onto an imposter site. Once on the imposter website, the user's browser is disabled and the user is shown advertising or other information and cannot easily access their intended website due to the blocks presented by the hacker. These types of attacks pose the same risks as other infiltration attack methods, yet are much easier to carry out, and even the most advanced encryption technologies will not guarantee success against a potential breach.

Remote internet voting could lead to lack of privacy and coercion

We currently cast our ballots in a private polling booth so that our vote remains secret, even to the workers at the polling place. Remote internet voting, however, is inherently insecure as voters will vote from home, work, the internet café or any other place in which a computer is accessable.

At a traditional polling place, election officials control the infrastructure and the environment of the voting procedure, thereby virtually guaranteeing the security of the process. Remote internet voting, however, depends on a number of factors outside the election officer's control, such as whether the voter's operating system is supported by the proper software, whether the voting system can properly authenticate that the person attempting to vote is a legitimate voter who has not previously voted in the election, and other, non-technical issues, such as pressure from outside influences which may coerce or compel 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 might occur with an onlooking supervisor urging the employee to vote in a certain way with threat of sanction.

Remote internet voting would alter the established voting culture

While it is true that a growing number of ballots are cast in pre-poll voting centres or by post instead of at a polling place, Australians celebrate democracy through free and fair elections and have confidence in a system that has repeatedly proven its merits as an electoral system. The act of families gathering at a polling place 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. The shared celebration of voting on a nominated day should not be discarded lightly. While social science issues are more abstract than the security or cost-related concerns, the effect of internet voting on the community is a real burden to implementing internet voting as its advent on a widespread scale could affect the voting culture quite substantially.

Opponents to remote internet voting claim its implementation will destroy the social cohesion of Australian voters and produce the negative result of a divided society. The current system of voting is seen to promote the community over the individual, where the civic duty of voting is ritualistically followed by all citizens, citizens who for one moment in time enjoy equal standing with all others, regardless of situation, wealth, colour, beliefs, or education. On the other hand, if one segment of society (those with internet access, statistically shown to be mainly middle to upper class, well educated people of European descent) opt to vote remotely instead of physically going to the polling place, the community ideals of voting disappear. For those reasons, a move to online voting would have to be done in such a way as to not undermine the significance of the event and the sense of community created by voting.

Opponents of remote internet voting also insist that its implementation could create other equality issues. Numerous studies have discovered that voters are less likely to make mistakes with e-voting than traditional voting methods, resulting in fewer informal votes. 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. However, as long as remote internet voting is an alternative to, and not a replacement of, polling place voting, election officials should avoid questions of fundamental inequities which remote internet voting could produce.

The costs of implementing a remote internet voting scheme are substantial

A functional internet voting system may offer substantial long-term savings over the present system of voting. For instance, a remote voting system would remove the need to maintain as many polling places on election day, thus reducing the number of polling place staff and training costs associated with such staff. In addition, the introduction of remote internet voting would substantially reduce the amount of money spent on the voting infrastructure by reducing the printed number of voting materials as well as decreasing the time and resource burden of maintaining security over and accurately counting the votes.

While the potential costs savings in the future appear substantial, the costs of initiating an internet voting regime is considerable. For instance, the initial outlays of developing or purchasing reliable and safe remote e-voting technology would be an expensive venture in and of itself, but when one figures in the cost of hiring technical experts to monitor the system and training staff, the start-up costs grow significantly and could even prove prohibitive. Once the initial outlays are out of the equation, however, remote internet voting may offer substantial savings over the present system of voting. Studies must be conducted to calculate the long-term costs of internet voting to ascertain if the system is cost-effective to implement.

Conclusion

Despite the inherent weaknesses present in remote internet voting, the public continues to clamour for convenience in the present voting system and many see remote internet voting as providing that convenience. It may be only a matter of time before Australian politicians follow in the footsteps of their British counterparts and decide to take up the campaign and actively promote internet voting. When that time comes, Australian election officials need to be armed with research and information so they can make informed, responsible decisions on the future of our democracy.

Remote internet voting could bring numerous advantages to the voting process, and the point of this article is not to summarily discount internet voting as a long-term option. Instead, this article attempts to point out some concerns regarding internet voting which the public and election officials need to consider before advocating its implementation.

The future of voting in Australia is unquestionably going to involve some form of e-voting. With properly funded and managed studies, research and trials, the transition could be smooth and the people will remain confident in the system. But if the transition happens too quickly, or without properly addressing the legitimate concerns of some opponents of e-voting, Australia puts its democratic process at risk due to the possibility of electoral failure.

Bryan Mercurio
is Electoral Law Project Director at the Gilbert + Tobin Centre for Public Law, UNSW.