Internet Voting Outside the United States

A dozen nations have explored the use of online voting since 2000 and we profile the experience of six countries on this page: Australia, Canada, Estonia, Finland, France and Norway. These examples are often presented as reasons why the United States should be able to deploy Internet voting – "if they are doing it, why aren't we?" It is worth noting that while some of the countries using the technology believe it has been successfully deployed, this may be due to an abundance of optimism about the challenge of securing such elections. Computer technology lends itself to undetected subversion and where problems have been too obvious to ignore some countries have discontinued piloting or using online voting for the present.

Unsolved problems with internet security make the electronic transmission of voted ballots too vulnerable to attack and too unreliable to be deployed today in our public elections. Beyond the threat of hacking or error, internet voting cannot provide an adequate means of independently verifying vote totals, which will inevitably erode public confidence in the announced results of close or disputed elections. While some promising end-to-end voter verifiable systems are under development, current commercially available technology is untested, proprietary, too vulnerable, and incapable of overcoming these fundamental vulnerabilities.

Australia

Australia has experimented with pilots of Internet voting technologies, most recently in New South Wales in 2011. An assessment of the NSW program noted that there was a significant problem with mis-recorded votes, where votes were recorded as an alphabetic letter rather than as the required digits. Those votes were not counted, and voters were not able to re-vote. Other problems pertained to voter authentication, including a circumstance in which voters using truncated ID numbers (fewer digits than official ID numbers were required to have) were able to log in and vote. Using ID numbers was meant to anonymise the voters, but because the system failed to properly separate ID numbers from votes or voters, the New South Wales Electoral Commission was able to trace the votes to the voters using the incorrect ID numbers, completely contravening the country's anonymity requirement.

Post-Implementation Review of the iVote Project (Price Waterhouse Coopers, 2015)
The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election (Halderman and Teague, 2015)
Problems with the iVote Internet Voting System (Computing Research and Education Association of Australasia, 2012)
Post Implementation Report (Elections NSW, 2011)
iVote Report (Allen Consulting Group, 2011)

Canada

Canada has been contemplating online voting for several years in Federal, Provincial and Municipal elections. In 2011 the British Columbia Elections Commission produced a paper recommending against online voting (see below), yet some jurisdictions have continued to move forward. Indeed, a primary election in 2012 was disrupted by hackers. Incidentally, days later a non-governmental election in Hong Kong was also attacked. In 2013 Elections Canada, the independent, non-partisan agency responsible for conducting federal elections and referendums in that nation, reported it is holding off on further experimentation with Internet voting until at least after 2015.

Recommendations Report to the Legislative Assembly (Independent Panel on Internet Voting, BC, 2014)
Security Assessment of Vendor Proposals (City of Toronto, 2014)
Web Accessibility (WGAC 2.0) Evaluation (City of Toronto, 2014)
Status Update – Internet Voting Service for PErsons with Disabilities for the 2014 Municipal Election (City of Toronto, 2014)
Internet Voting for Persons with Disabilities – Demonstration Script (City of Toronto, 2013)
RFP for Internet Voting (City of Toronto, 2013)
Scytl Agreement (City of Toronto, 2014)
Scytl Statement of Work – redacted (City of Leamington, 2014)
Scytl Statement of Work – unredacted (City of Leamington, 2014)
Dominion Statement of Work (City of Brockton, 2014)
Internet Voting Discussion Paper (Elections BC, 2011)
Internet Voting Report (Delvinia, 2004)

Estonia

Estonia began an internet voting program in 2005. In Estonia, where now 24% of voters use the Internet voting system, all citizens have a smart ID card, enabling voter authentication in a way we are unable to duplicate for an online voting system in the US. (Citizens in the U.S. do not have such a national ID system nor any similar public key infrastructure.) Authenticating the voter is only one challenge, however. The Estonia system was evaluated by The Organization for Security and Cooperation in Europe / Office for Democratic Institutions and Human Rights (OSCE/ODIHR) after their team carried out an observation mission in 2011. They described a number of security problems, including lack of adequate protection of anonymity or privacy of the ballots. A Finnish technologist familiar with the region reports from a 2013 trip there that so far most investigation of their Internet voting system has been done with a low level of technological proficiency.

A petitioner sued to invalidate the electronic results in the 2011 Estonian election, on the basis that it was possible for a virus to block submission of an Internet vote without the voter's knowledge, and made a successful demonstration of such a vulnerability to the Court. Nonetheless, because there was no other mechanism to evaluate the reported result, the Court found no evidence that the reported result was inaccurate, and rejected the legal challenge. (There are more interesting legal aspects if you are interested!) The Estonian system also fails

to provide for use by voters who speak a language other than Estonian.

Security Analysis of the Estonian Internet Voting System (Halderman, Hurst, Kitcat, et al, 2014)
Report on 2011 Estonian Parliament Elections (Office for Democratic Institutions and Human Rights, 2012)

Finland

Finland explored the use of a kiosk-based online voting system, which offers increased protection against coercion, and reduces somewhat the risk of some forms of malware. The U.S. Election Assistance Commission and a number of computer scientists studying the issue believe that the most likely prospect for online voting with any measure of security would be a kiosk-based system. However, early experiments with a kiosk-based system have shown scalability issues. More notably for the US, the systems being deployed and used today in the U.S. are *not* kiosk-based, lacking even the partial mitigations a kiosk system might offer. Due to significant flaws in the system resulting in lost votes, Finland's Supreme Administrative Court in 2009 annulled results of Finnish 2008 municipal election and called for a re-vote on a paper ballot system.

A Report on the Finnish E-Voting Pilot (Electronic Frontier Finland, 2009)
Report on Finnish E-Voting Pilot (Council of Europe, 2008)

France

France conducted an online primary in 2014, its first, using a system touted as secure, but journalists from the news site Metronews proved that it was easy to breach the allegedly strict security of the election and vote several times using different names, throwing the outcome into doubt.

Norway

Norway has been experimenting with a system developed by a Spanish company, Scytl. *(The same company's system was piloted in the US in 2008 in Okaloosa County, and reviewed here. In that test, a physical copy of the voter's choices, reviewed by each voter, was produced, in addition to the electronic copy. This enabled an audit of the system, but that feature is nearly always absent with Internet voting systems.)*

A "low-effort review of the source code" of Norway's system was conducted by experts from the Norwegian Computing Center and the Norwegian University of Science and Technology, finding even at a rudimentary glance "significant problems with coding style, security and correctness."

We do not know if any mitigating improvements have been made to date, but the problems found had the potential for altered outcomes. In June, 2014 the Norwegian Government announced that it would no longer pursue internet voting pilot projects.

Public Review of E-Voting Source Code (Tapir Akademisk Forlag, 2011)

Other Countries

Other European countries have experimented with electronic or Internet voting and have elected to discontinue its use. In **Spain**, an election for a "referendum in the Spanish city of Barcelona encountered problems in relation to voter identification and identity theft, with a prominent voter finding that someone had already logged on with his authentication details and cast a ballot for him," as reported in this comprehensive 2012 International Foundation for Electoral Systems (IFES) report about Internet and electronic voting. In August 2014, Arnis Cimdars, chairman of Latvia's Central Electoral Commission (CVK) said that electronic voting was not secure enough to allow it to be used in Latvian elections, noting According to our experts, it is not possible for us with current technology. We have some mental reservations about this method of voting, too… at the moment it is not possible to ensure the anonymity and security of this method of voting, so I don't think it will happen very soon."