Lessons in trust from America's experience with electronic voting

January 3 2017, by Roland Wen And Richard Buckland

It reads like a Hollywood movie. Elite hackers, allegedly sponsored by the Russian government, infiltrate the computer systems of the Democratic National Committee. Thousands of emails are stolen and published by WikiLeaks.

And then, suspected Russian hackers attack the voter registration systems of more than 20 American states. Up to 200,000 voter records are stolen from one system.

These seemingly far-fetched cyberattacks actually happened in the lead-up to the US presidential election. The country's intelligence community believes these attacks were "intended to interfere with the US election process", or perhaps even to influence the election outcome.

While there is as-yet no evidence of cyberattacks during the election itself, several states used insecure electronic election systems. This has resulted in many voters losing trust in the electoral process and petitions for recounts.

But would recounts be sufficient to rebuild trust? And what can Australia learn about maintaining trust in the electoral process as technology becomes widespread?

Recounts in the US

Green Party candidate Jill Stein and election security experts called for full manual recounts of the original paper ballots for the presidential election in the states of Wisconsin, Pennsylvania and Michigan. Doing it manually would have eliminated the potential for compromised or defective systems to affect the recount.

However, legal action stopped the recounts from going ahead in Pennsylvania and Michigan. And Donald Trump's margin of victory increased in Wisconsin following the recount there.

Each county in Wisconsin decided separately on which recount method it used. This depended on whether voting was by voting machines with audit printouts or by paper with automated scanning and counting.

Voting machines in Wisconsin produced paper audit trails as voters voted. For these systems the paper audit trail is manually counted.

In optical scan voting, voters filled out their votes on optical scan paper ballots, which were then automatically scanned and computer-counted. To recount those, a county must choose to either switch to manually counting the paper ballots, or repeat the automated scan and computer count process.

Simply repeating the automated scan and count process has fundamental problems; fraud and error in the initial count might simply be repeated in the recount. A compromised scanner could make the same fraudulent changes to the tally. A defective scanner could experience the same software or hardware errors – say, by systematically misinterpreting particular ballots.

A reliable recount in Pennsylvania would have been even more difficult. Its voting machines don't print audit trails, and so there is no way to recount or audit the votes cast using them.

Stein's legal action called for the Pennsylvania recount attempt to include a forensic audit to examine voting machines for evidence of tampering. But such an audit could still fail to detect many attacks that hide their tracks.

Consequently, had they been allowed to do a recount, electoral officials would have faced considerable difficulty in providing strong public reassurance that fraud and error can be detected and rectified.

Lessons for Australia

Elections worldwide are becoming increasingly dependent on technology. But, typically, the electronic systems adopted suffer from weak transparency and scrutiny even when the outcome is challenged. This is creating serious risks that citizen trust in electoral processes will be damaged.

Australia also faces these risks. The Senate vote capture system used in the 2016 federal election shares many of the same vulnerabilities as the optical scan voting systems used in US elections.

These risks could be more serious in Australia, because manual recounts would likely be insurmountably costly and slow for complex Senate elections. Electronic data capture and counting are necessary to carry out large-scale preferential counting in Australia.

So, although Australian handwritten ballots provide a paper trail, there is no practical manual fallback alternative for counting them.

Despite these risks, technology also offers the potential to increase accuracy and so actually improve trust. In elections that use simpler preferential counting methods than the Senate and are much smaller in scale, manual counting has traditionally been found to be error-prone.

For example, the recent manual count for the byelection in the NSW seat of Orange (a total of about 50,000 votes) was found to have an error of 75 votes in the "final count" versus the recount. Significantly, this error was larger than the losing margin. These manual errors had continued even after another error in an earlier count had a different candidate winning by 66 votes.

What's missing for elections using technology are careful transparency and scrutiny measures to help mitigate these risks and build trust.

A first step to building trust is to convincingly demonstrate that election systems satisfy the high level of security, reliability and quality appropriate for failure-critical national infrastructure. This is particularly crucial when there can be no practical manual fallback as a Plan B.

For example, a basic transparency measure is to make the design, implementation, testing, operation and auditing of the system and procedures available for broad scrutiny. A basic scrutiny measure is to engage a wide range of experts to rigorously examine the system and procedures before, during and after the election to detect defects, vulnerabilities and other problems.

Building trust also requires the system and procedures to be designed to make fraud and error evident – not just to assert they are unlikely.

One practical scrutiny measure for Senate elections would be to check a random sample of the paper ballots against the output of the scanning machines used in the counting. This would help expose failures in the vote capture system.

A transparency measure already used in Senate elections is to publish the electronic votes so anyone can check the output of the electronic counting program. Implementing both measures would provide stronger public assurance for the entire Senate electronic vote capture and counting process.

The lesson for Australia is the importance of carefully considering what are the appropriate transparency and scrutiny safeguards to build into our systems, in advance of scandals, to ensure continued public trust in the electoral process.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Lessons in trust from America's experience with electronic voting (2017, January 3) retrieved 13 May 2024 from https://phys.org/news/2017-01-lessons-america-electronic-voting.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.