Andrea Gyger

From: von Spakovsky, Hans <Hans.VonSpakovsky@heritage.org>
Sent: Tuesday, July 14, 2015 2:30 PM
To: SoS Rulemaking
Subject: 8 CCR 1505-1
Attachments: Heritage-Internet voting.pdf

Please find attached a policy paper on the dangers of Internet voting, including the electronic delivery of voted ballots.

Hans von Spakovsky
Manager, Election Law Reform Initiative and Senior Legal Fellow
The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
202-608-6207
heritage.org

The Heritage Foundation

BACKGROUNDER

No. 3034 | JULY 14, 2015

The Dangers of Internet Voting

Hans A. von Spakovsky

Abstract

Those who believe that it is "possible given current technology" to create a secure online voting system are dangerously mistaken. According to computer experts, Internet voting is vulnerable to cyber-attack and fraud—vulnerabilities inherent in current hardware and software, as well as the basic manner in which the Internet is organized—and it is unlikely that these vulnerabilities will be eliminated in the near future. Internet voting, or even the delivery by e-mail of voted ballots from registered voters, would be vulnerable to a variety of well-known cyber-attacks, any of which could be catastrophic. Such attacks could even be launched by an enemy agency beyond the reach of U.S. law and could cause significant voter disenfranchisement, privacy violations, vote buying and selling, and vote switching. The biggest danger, however, is that such attacks could be completely undetected.

Those who believe that "voting online is the future" or that it is "possible given current technology" to create a secure online voting system are dangerously mistaken.[1] According to computer experts, Internet voting is vulnerable to cyber-attack and fraud—vulnerabilities inherent in current hardware and software, as well as the basic manner in which the Internet is organized. It is unlikely that these vulnerabilities will be eliminated at any time in the near future.

State legislators and secretaries of state who are considering implementing Internet voting, or even the delivery by e-mail of voted ballots from registered voters, should reconsider such measures. These programs would be vulnerable to a variety of well-known cyber-attacks, any of which could be catastrophic. Such

Key Points

- Although being able to cast a ballot from your home computer, like being able to order and buy products and services through online Internet transactions, might make voting more convenient, the extraordinary security problems of such a remote Internet voting system present an unacceptable risk to election integrity.
- The overwhelming conclusion of computer experts is that those security vulnerabilities are inherent in the architecture and organization of the Internet and the software and hardware in common use today.
- Without major technological changes, there is almost no possibility that a secure Internet voting system can be designed for the foreseeable future.
- State legislators and secretaries of state who are considering implementing Internet voting, or even the delivery by e-mail of voted ballots from registered voters, should reconsider such measures.
- Internet voting is definitely a technology whose time has not come—and may never come.

This paper, in its entirety, can be found at **http://report.heritage.org/bg3034**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

attacks could be "launched by anyone from a disaffected lone individual to a well-financed enemy agency outside the reach of U.S. law."[2] They also "could result in large-scale, selective voter disenfranchisement," privacy violations, vote buying and selling, and vote switching "even to the extent of reversing the outcome of many elections at once…."[3] The biggest danger, however, is that such attacks "could succeed and yet go completely undetected."[4]

Expert Analyses of Internet Voting

California. Convened by former California Secretary of State Bill Jones, the California Internet Voting Task Force performed the first serious evaluation of Internet voting. The task force used its proximity to Silicon Valley—the heart of the U.S. computer industry—to involve front-line computer experts in its evaluation of the feasibility of and security issues involved in Internet voting. Those experts came from a variety of software and hardware companies and institutions including Compaq Computers, Oracle, Cisco Systems, and the California Institute of Technology.

In its final report, issued on January 18, 2000, the task force defined Internet voting as "an election system that uses electronic ballots that would allow voters to transmit their voted ballot to election officials over the Internet."[5] It concluded that "[p]otential criminal electronic attacks on computer software, such as destructive 'viruses' or 'Trojan Horse' software, create a serious threat to Internet voting."[6] The group further believed that "additional technical innovations are necessary before remote Internet voting can be widely implemented…."[7]

National Science Foundation. In 2001, a report commissioned by the National Science Foundation (NSF) reached a similar conclusion. The experts convened by the NSF found that although remote Internet voting would maximize convenience, "it also poses substantial security risks" that "current and near-term technologies are inadequate to address." In fact, "remote Internet voting systems pose significant risk to the integrity of the voting process, and should not be fielded for use in public elections until substantial technical and social science issues are addressed."[8]

The NSF report also noted that "Internet-based voter registration poses significant risk to the integrity of the voting process, and should not be implemented for the foreseeable future." It argued that the "voter registration process is already one of the weakest links in our electoral process" and that "introduction of Internet-based registration without first addressing the considerable flaws in our current system would only serve to greatly exacerbate the risks to which we are already exposed." The NSF report concluded that:

> While information already in the domain of election officials may be updated remotely, given appropriate authentication protocols, initial registration conducted online cannot establish the identity of the registrant without the transmission of unique biometric (fingerprint or retinal scan) data and an existing database with which to verify the data. Online registration without the appropriate security infrastructure would be at high risk for automated fraud (i.e., the potential undetected registration of large numbers of fraudulent voters).[9]

[1] Markos Moulitsas, "Voting Online Is the Future," *The Hill*, May 13, 2014, http://thehill.com/opinion/markos-moulitsas/206047-markos-moulitsas-voting-online-is-the-future (accessed July 6, 2015).

[2] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, January 20, 2004, p. 2, http://www.servesecurityreport.org/ (accessed July 6, 2015).

[3] Ibid.

[4] Ibid.

[5] California Internet Voting Task Force, *A Report on the Feasibility of Internet Voting*, January 2000, p. 2, http://elections.cdn.sos.ca.gov/ivote/final_report.pdf (accessed July 6, 2015).

[6] Ibid., p. 4.

[7] Ibid., p. 2.

[8] Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, March 2001, p. 2, http://www.verifiedvoting.org/wp-content/uploads/downloads/NSFInternetVotingReport.pdf (accessed July 6, 2015). The workshop was sponsored by the National Science Foundation, conducted in cooperation with the University of Maryland, and sponsored by the Freedom Forum.

[9] Ibid., pp. 2–3.

Pentagon Internet Voting Project. Because of the severe problems that overseas military and civilian personnel experience when voting, Congress directed the Federal Voting Assistance Program (FVAP) office at the U.S. Department of Defense to develop an Internet voting system pilot project for use in the 2004 federal election.[10] FVAP is responsible for administering the Uniformed and Overseas Citizens Absentee Voting Act, a federal law that requires all states to "permit absent uniformed services voters and overseas voters to use absentee registration procedures and to vote by absentee ballot in general, special, primary, and runoff elections for Federal office."[11]

Military voters in particular have an unacceptably high disenfranchisement rate that is caused by the long delays associated with mailing absentee ballots to and from remote, overseas locations and war zones.[12] The proposed Secure Electronic Registration and Voting Experiment (SERVE) would have allowed remote Internet registration and voting by overseas military and civilian personnel in 50 counties in seven states (Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington), starting with the 2004 South Carolina primary, potentially handling up to 100,000 votes.[13]

However, the SERVE project was canceled after four computer experts—invited by the Pentagon to review the Internet voting system—issued a devastating report.[14] Their analysis, which pointed out vulnerabilities that apply to Internet voting in general and not just to the specifics of the SERVE system, echoed the earlier findings of the California and NSF task forces. These experts concluded that SERVE, an Internet- and PC-based system, would be vulnerable to cyber-attacks including "insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks on voter PCs, etc."[15]

While it was not possible to estimate the probability of a successful cyber-attack on any one election, the experts pointed out that the attacks they were "most concerned about are quite easy to perpetrate." In fact, "there are kits readily available on the Internet that could be modified or used directly for attacking an election." The experts pointed out "the obvious fact that a U.S. general election offers one of the most tempting targets for cyber-attack in the history of the Internet, whether the attacker's motive is overtly political or simply self-aggrandizement."[16]

One of the most serious problems inherent in any remote Internet voting system was that the vulnerabilities found by the computer experts could not be fixed "by design changes or bug fixes to SERVE." In fact, "these vulnerabilities are fundamental in the architecture of the Internet and of the PC hardware and software that is ubiquitous today." The experts concluded that the vulnerabilities they found could not be "eliminated for the foreseeable future without some unforeseen radical breakthrough" and that "it is quite possible that they will not be eliminated without a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet."[17] No such "wholesale redesign" of the Internet or hardware/software has occurred since the SERVE analysis was issued.

After the Pentagon cancelled the SERVE project, the National Defense Authorization Act of 2005 amended the 2002 provision that had authorized the establishment of SERVE. It directed the Defense Department to implement another Internet voting

[10] National Defense Authorization Act of 2002, §1604.

[11] 42 U.S.C. 1973ff-1(1).

[12] Hans A. von Spakovsky and M. Eric Eversole, "America's Military Voters: Re-enfranchising the Disenfranchised," Heritage Foundation *Legal Memorandum* No. 45, July 28, 2009, revised and updated March 9, 2010, http://www.heritage.org/research/reports/2009/07/americas-military-voters-re-enfranchising-the-disenfranchised. This is a particularly difficult problem for Navy personnel on fleet deployments.

[13] News release, "Security Experts Urge U.S. to Abandon Internet Voting Plan," Johns Hopkins University, January 21, 2004, http://www.servesecurityreport.org/press.pdf (accessed July 6, 2015).

[14] Jim Garamone, "Pentagon Decides Against Internet Voting This Year," American Forces Press Service, February 6, 2004, http://www.defense.gov/news/newsarticle.aspx?id=27362 (accessed July 6, 2015).

[15] Jefferson et al., *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, p. 2.

[16] Ibid.

[17] Ibid., pp. 2–3.

project if and when the U.S. Election Assistance Commission adopts standards developed by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce that would ensure the safe, secure transmission of electronic ballots.[18]

NIST, however, has been unable to establish that secure Internet voting is feasible, because "remote electronic absentee voting from personally-owned devices face a variety of potential attacks on voters and voters' personal computers" that are "commonplace on the Internet today" and "extremely difficult to protect against."[19] As a result, Congress repealed the directive for an Internet voting demonstration project in the 2015 National Defense Authorization Act.[20]

Computer Technologists' Statement on Internet Voting. In 2008, 32 respected computer scientists from universities across the country, including Stanford University, Princeton University, John Hopkins University, Carnegie Mellon University, Indiana University, Rice University, Purdue University, and the University of Texas at Austin, issued a statement about the vulnerabilities of Internet voting, listing the technical challenges to implementing a safe and secure system.[21]

These scientists warned that there are "serious, potentially insurmountable, technical challenges" to transmitting votes over the Internet in a secure and verifiable manner. They recommended that Internet voting not be adopted until and unless "these technical challenges have been overcome." The challenges listed included:

- Preventing malicious software, firmware, or hardware that can change, fabricate, or delete votes, deceive the user in myriad ways including modifying the ballot presentation, leaking information about votes to enable voter coercion, preventing or discouraging voting, or performing online electioneering;
- Stopping denial of service attacks from networks of compromised computers (called "botnets"), causing messages to be misrouted, and many other kinds of attacks;
- Finding a strong mechanism to prevent undetected changes to votes not only by outsiders, but also by insiders such as equipment manufacturers, technicians, system administrators, and election officials who have legitimate access to election software and data;
- Providing a reliable, unchangeable voter-verified record of votes that is at least as effective for auditing as paper ballots without compromising ballot secrecy; and
- Designing a system that is reliable and verifiable even though Internet-based attacks can be mounted by anyone anywhere in the world.

The problem with all of these challenges, according to the experts, is that neither the software nor the hardware currently exists to overcome these challenges. This problem is exacerbated by the Internet's existing architecture, which is vulnerable to all types of cyber-attacks that are "difficult or impossible to trace back to their sources." Because of these problems, "there is ample reason to be skeptical of Internet voting proposals," and Internet voting would present "an extraordinary and unnecessary risk to democracy." The computer scientists even recommended against "pilot studies" because the "apparent 'success' of such a study absolutely cannot show the absence of problems that, by their nature, may go undetected."[22]

[18] H.R. 4200, Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, 108th Cong., § 567, 2005, http://www.gpo.gov/fdsys/pkg/BILLS-108hr4200enr/pdf/BILLS-108hr4200enr.pdf; see also letter from Joe Wilson, Chairman, Military Personnel Subcommittee, U.S. House Committee on Armed Services, to Jon T. Rymer, Inspector General, U.S. Department of Defense, June 24, 2014.

[19] Nelson Hastings, Rene Peralta, Stefan Popoveniuc, and Andrew Regensheid, *Security Considerations for Remote Electronic UOCAVA Voting*, U.S. Department of Commerce, National Institute of Standards and Technology, February 2011, p. 59, http://www.nist.gov/itl/vote/upload/NISTIR-7700-feb2011.pdf (accessed July 6, 2015).

[20] Sec. 593: "Section 1604 of the National Defense Authorization Act for Fiscal year 2002 (Public Law 107-107; 52 U.S.C. 20301 note) is repealed."

[21] "Computer Technologists' Statement on Internet Voting," 2008, http://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf (accessed July 6, 2015).

[22] Ibid.

In addition to problems with remote Internet voting, the Verified Voting Foundation (VVF), which includes experts who were involved in the California, NSF, and SERVE task forces and who helped to organize the Computer Technologists' Statement on Internet Voting, points out problems with the security of an Internet-related measure that 30 states, including Alaska and Arizona, have adopted: the electronic delivery of voted ballots via e-mail attachments.[23]

The VVF states what should be obvious to every computer user from their everyday experiences: The personal computers used by voters to send e-mails are "easily and constantly attacked by viruses, worms, Trojan Horses and spyware." Indeed, once a voted ballot is e-mailed by a voter to election officials:

> [I]t moves between many different servers located all over the planet, and is subject to compromise by anyone with access to any of those machines. And the election official on the receiving end has no way to know if the voted ballot she received matches the one the voter originally sent, no matter how well secured their County computer services may be, and no matter how much has been spent licensing software and upgrading their systems.[24]

NIST agrees with that assessment. In a 2011 report, it warned that election officials considering the use of e-mail transmission of election materials such as ballots "should carefully consider the security limitations of e-mail" because e-mails can be "intercepted, read, and modified in transit." They also can be "easily forged to make it look like [the e-mail] was sent from another individual."[25]

David Jefferson of the Lawrence Livermore National Laboratory, who chaired the Technology Committee of the California Internet Voting Task Force, calls e-mail and fax transmission "by far the most dangerous forms of voting ever implemented in the U.S."[26] Yet election officials like Colorado Secretary of State Wayne Williams, who claimed that any concern that these voting systems are hackable is a "nonstarter," continue to demonstrate a dangerous lack of knowledge regarding these critical security issues.[27]

Experiences with Internet Voting

Washington, D.C. In 2010, the District of Columbia was so confident in the security of its Internet voting pilot project, which would have allowed overseas absentee voters to cast their ballots using a website, that it set up a mock election and challenged hackers to test the system.[28] Within 36 hours, a computer science professor at the University of Michigan in Ann Arbor and his students broke into the system, changed the results of the mock election, and "gained near-complete control" of the election server: "We successfully changed every vote and revealed almost every secret ballot. Election officials did not detect our intrusion for nearly two business days—and might have remained unaware for far longer had we not deliberately left a prominent clue."[29]

The "prominent clue" that Professor Alex Halderman left was a modification of the "Thank You" page at the end of the voting process for a voter using the system that played the University of Michigan fight song. Despite that clue, officials became aware of the intrusion only because an e-mail on a mailing list that election officials monitored inquired, "does anyone know what tune they play for successful

[23] Verified Voting Foundation, "Internet Voting," http://www.verifiedvoting.org/resources/internet-voting/ (accessed July 6, 2015).

[24] Ibid.

[25] Andrew Regensheid and Geoff Beier, *Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters*, U.S. Department of Commerce, National Institute of Standards and Technology, September 2011, p. 12, http://nist.gov/itl/vote/upload/nistir7711-Sept2011.pdf (accessed July 6, 2015).

[26] Greg Gordon, "Pentagon Unit Pushed Email Voting for Troops Despite Security Concerns," McClatchy Newspapers, November 4, 2012, http://www.mcclatchydc.com/news/politics-government/election/article24739735.html (accessed July 6, 2015).

[27] Letter from Wayne W. Williams, Secretary of State, Colorado, to Honorable Sponsors of HB15-1130, April 17, 2015.

[28] Sarah Wheaton, "Voting Test Falls Victim to Hackers," *The New York Times*, October 8, 2010, http://www.nytimes.com/2010/10/09/us/politics/09vote.html?_r=1 (accessed July 6, 2015).

[29] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, "Attacking the Washington, D.C. Internet Voting System," Proceedings of 16th Conference on Financial Cryptography and Data Security, February 2012, p. 1 (accessed July 6, 2015).

voters?"[30] The issue was not just that Halderman and his students were able to take control of the Internet voting system; they were also able to hide their presence in the terminal server from the election officials who were supposedly monitoring the security of the system.

Halderman was also able to detect attempted intrusions by "several other attackers," including IP addresses in Iran, New Jersey, India, and China. Thus, as the Washington project demonstrates, the danger of an organized attack by a "well-financed enemy agency" is not a matter of mere speculation, but a likely reality. For instance, the Chinese Communist government has a special hacking unit of "cyber warriors"—People's Liberation Army Unit 61398—that American officials suspect is responsible for numerous cyber-attacks on government and commercial networks in the U.S.[31] In recent years, this unit has increased its focus on "the critical infrastructure of the United States—its electrical power grid, gas lines and waterworks."[32] These hackers are focused "not just on stealing information, but [on] obtaining the ability to manipulate" that critical infrastructure.[33]

Anyone who doubts that an Internet voting system would be targeted by organized, government-sponsored hackers like PLA Unit 61398 is not being realistic. The ability to change or manipulate the outcome of an American election through the Internet would just be too tempting a target—particularly because no legal process here could reach hackers ensconced abroad and under the protection of a hostile government. The power of these hackers was demonstrated recently by what some officials are calling "the largest known theft of government data in history" when they managed to steal the personal records of federal government employees, federal retirees, and former federal employees from the U.S. Office of Personnel Management.[34]

Estonia. In 2005, Estonia became the first country to offer Internet voting in a national election. It has been used seven times in local and national elections, according to a critical analysis published in 2014. University of Michigan Professor Alex Halderman and his students conducted a thorough review of the system and then prepared an analysis of the Estonian system's vulnerabilities that identified major security risks and recommended its immediate termination. Halderman and his team "observed operations during the October 2013 local elections, conducted interviews with the system developers and election officials, assessed the software through source code inspection and reverse engineering, and performed tests on a reproduction of the complete system in our laboratory."[35]

Their research showed that the system's numerous security lapses created an "attractive target for state-level attackers, such as Russia." These attackers, as well as dishonest election officials, "could change votes, compromise a secret ballot, disrupt voting, or cast doubt on the legitimacy of the election process."[36] The system had such "serious procedural and architectural weaknesses" that "attackers could undetectably alter the outcome of an election," a shocking finding that the National Election Committee of Estonia refused to acknowledge. Unfortunately, Estonia continues to use this unsecure, dangerous Internet voting system.

[30] Ibid., p. 8.

[31] David Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, February 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=0 (accessed July 6, 2015).

[32] Ibid.

[33] Ibid.

[34] Devlin Barrett, Danny Yadron, and Damian Paletta, "U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say," *The Wall Street Journal*, June 5, 2015, http://www.wsj.com/article_email/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888-lMyQjAxMTE1NjA2NDYwMzQ2Wj (accessed July 6, 2015); Ken Dilanian, "Union Says All Federal Workers Fell Victim to Hackers," *The Washington Times*, June 12, 2015, http://www.washingtontimes.com/news/2015/jun/12/union-says-all-federal-workers-fell-victim-hackers/?page=all (accessed July 6, 2015).

[35] Drew Springall, Travis Finkenhauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman, "Security Analysis of the Estonian Internet Voting System," Proceedings of the 21st ACM Conference on Computer and Communications Security, November 2014, https://estoniaevoting.org/findings/paper/ (accessed July 6, 2015).

[36] Ibid.; see also news release, "Independent Report on E-voting in Estonia," May 12, 2014, https://estoniaevoting.org/press-release/ (accessed July 6, 2015).

Unlike Estonia, neighboring Latvia does not have Internet voting. Arnis Cimdars, chairman of Latvia's Central Electoral Commission, has said that "with current technology" it is "not possible to ensure the anonymity and security of this method of voting."[37]

France. In 2013, France used an Internet voting system for the first time in a Parisian mayoral primary. The backers of the system, just like election officials in Washington, D.C., claimed that it was "fraud-proof" and "ultra secure." However, reporters 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."[38] One of the journalists voted five times, including once in the name of former French President Nicolas Sarkozy.

Norway. Norway implemented a limited Internet voting system for municipal elections in 2011 and 2013 but cancelled the project in 2014, citing security concerns and the government's conclusion that, contrary to expectations, the new system had not improved turnout. Specifically, Norway's Institute of Social Research said that there was "no evidence that the trial led to a rise in the overall number of people voting nor that it mobilized new groups, such as young people, to vote."[39] Even just a "low-effort" review of the system by computer experts from the Norwegian Computing Center and the Norwegian University of Science and Technology found "significant problems" with security, among other things, to the extent that the experts said the software did "not have acceptable quality for use in an e-voting system."[40]

Canada. In 2014, an independent review panel in British Columbia issued a report opposing "universal Internet voting." This report pointed out that while the Internet is used for "an increasing number of interactions (such as banking, shopping, dating, planning trips, and the like) with their own risks, voting over the Internet has a set of unique challenges that inevitably introduce a number of additional risks."[41] The report concluded that one of the biggest problems with Internet voting is the insecure nature of personal computers that "are already the target of malware, phishing attempts and other attacks."[42]

The malware that has been "developed for other purposes such as capturing credentials used for online banking and purchases can be used to record the voter's authentication credentials or track who an individual has voted for." It would also be possible to develop new malware "to target specific voting systems" in order to "alter how the ballot is marked" and to do so "without the voter's knowledge." Finally, as Norway experienced, the report concluded that "considerable research" shows that Internet voting would not increase turnout and "cause nonvoters to vote." Instead, it would simply be "used as a tool of convenience for individuals who have already decided to vote."[43]

When Toronto was considering Internet voting, two experts commissioned by the city filed a report reviewing the various proposals that had been submitted by voting vendors. The experts recommended against proceeding because none of the proposals provided "adequate protection against the risks inherent in internet voting."[44] Regrettably, Toronto has gone forward with a contract to develop Internet voting for the disabled despite the security vulnerabilities that any such system would present.

[37] *No E-Voting for Latvia Anytime Soon*, LSM.LV (Public broadcasting of Latvia) (August 6, 2014), http://www.lsm.lv/en/article/societ/society/no-e-voting-for-latvia-any-time-soon.a93774/.

[38] John Lichfield, "Fake Votes Mar France's First Electronic Election," *The Independent*, June 2, 2013, http://www.independent.co.uk/news/world/europe/fake-votes-mar-frances-first-electronic-election-8641345.html (accessed July 6, 2015).

[39] BBC, "E-voting Experiments End in Norway Amid Security Fears" June 27, 2014, http://www.bbc.com/news/technology-28055678 (accessed July 6, 2015).

[40] Bjarte M. Østvold and Edvard K. Karlsen, "Public Review of E-Voting Source Code: Lessons Learnt from E-vote 2012," October 2012, https://www.verifiedvoting.org/wp-content/uploads/2014/09/Norway-2012-Public-Review-of-E-voting-Source-Code-Lessons-Learnt-from-E-vote-2011.pdf (accessed July 6, 2015).

[41] Independent Panel on Internet Voting, *Recommendations Report to the Legislative Assembly of British Columbia*, February 2014, p. 1, http://www.internetvotingpanel.ca/docs/recommendations-report.pdf (accessed July 5, 2015).

[42] Ibid., p. 23. Malware is malicious software designed to interfere with a computer's normal functioning.

[43] Ibid., p. 12.

[44] Jeremy Clark and Aleksander Essex, *Internet Voting for Persons with Disabilities—Security Assessment of Vendor Proposals: Final Report*, February 14, 2014, p. 178, https://www.verifiedvoting.org/wp-content/uploads/2014/09/Canada-2014-01543-security-report.pdf (accessed July 6, 2015).

Other municipalities like Markham, Ontario, have proceeded with Internet voting, although Elections Canada, the federal government's election agency, dropped plans for a 2015 Internet voting pilot project because of budget cuts.[45]

Other Countries. As the Verified Voting Foundation points out, a number of other countries in Europe and elsewhere, such as Australia, have experimented with Internet voting, and many "have elected to discontinue its use" after significant security issues arose.[46] This includes Spain, which held a referendum in Barcelona in 2010 using the Internet. It is highly unlikely that Spain will implement Internet voting given that the Barcelona referendum "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."[47]

Australia held the world's largest-ever Internet voting deployment in the 2015 state election in New South Wales for the return of 280,000 ballots. Professor Alex Halderman and his team of computer experts analyzed the New South Wales system "and uncovered severe vulnerabilities that could be leveraged to manipulate votes, violate ballot privacy, and subvert the verification mechanism." According to Halderman, none of these vulnerabilities in the security of the Internet voting system was "detected by the election authorities" before Halderman and his team disclosed them, "despite a pre-election security review and despite the system having run in a live state election for five days."[48]

Halderman's report pointed out that "[a]t least one parliamentary seat was decided by a margin much smaller than the number of votes taken while the system was vulnerable." The Australian system was so flawed that an attacker could subvert the "voting session, expose the vote that voter intended to cast, substitute a different vote, and sidestep the verification mechanism so that last-minute manipulation was undetectable." Even worse, while implementing such an attack "required some skill," it would have required "no special knowledge that was not publicly available at the time."[49]

Comparison with E-Commerce

For those who point to the use of the Internet in the financial industry as proof that Internet voting would be secure, University of Maryland President C.D. Mote, Jr., who chaired the National Science Foundation committee on Internet voting, offers a compelling retort. Mote notes that voting "requires a much greater level of security then e-commerce—it's not like buying a book over the Internet." Moreover, "remote Internet voting technology will not be able to meet this standard for years to come."[50]

David Jefferson of the Lawrence Livermore National Laboratory says that people ask quite naturally, "If it is safe to do my banking and shopping online, why can't I vote online?"[51] The answer is that it is not actually safe "to conduct e-commerce transactions online." In fact, it is very risky, and online ecommerce fraud is a growing problem: The financial industry, including banks, credit card companies, and retailers, "lose[s] billions of dollars a year in online transaction fraud despite huge investments in fraud prevention and recovery." He adds that:

> The technical security, privacy, and transparency requirements for voting are structurally different from, and actually much more stringent than, those for ecommerce transactions.... People have

[45] Leslie MacKinnon, "Elections Canada Drops Plan for Online Voting Due to Cuts," CBC News, April 30, 2013, http://www.cbc.ca/news/politics/elections-canada-drops-plan-for-online-voting-due-to-cuts-1.1346268 (accessed July 6, 2015).

[46] Verified Voting Foundation, "Internet Voting Outside the United States," https://www.verifiedvoting.org/internet-voting-outside-the-united-states/ (accessed July 6, 2015).

[47] Jordi Barrat i Esteve, Ben Goldsmith, and John Turner, *International Experience with E-Voting*, International Foundation for Electoral Systems, June 2012, p. 17, http://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf (accessed July 6, 2015).

[48] J. Alex Halderman and Vanessa Teague, "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election," April 22, 2015, last revised June 5, 2015, p. 1, http://arxiv.org/pdf/1504.05646v2.pdf (accessed July 6, 2015).

[49] Ibid., p. 16.

[50] News release, "Internet Voting Is No 'Magic Ballot,' Distinguished Committee Reports," National Science Foundation, March 6, 2001, http://www.nsf.gov/od/lpa/news/press/01/pr0118.htm (accessed July 6, 2015).

[51] David Jefferson, "If I Can Shop and Bank Online, Why Can't I Vote Online?" Verified Voting Foundation, https://www.verifiedvoting.org/resources/internet-voting/vote-online/ (accessed July 6, 2015).

> the illusion that ecommerce transactions are safe because merchants and banks don't hold consumers financially responsible for fraudulent transactions that they are the innocent victims of. Instead the businesses absorb and redistribute the losses silently, passing them on in the invisible forms of higher prices, fees, and interest rates. Businesses know that if consumers had to accept those losses personally most online commerce would collapse. Instead, they routinely hide the losses, keeping the magnitude secret so the public is generally unaware. It's a good business strategy.[52]

According to Jefferson, it is not just that the "security, secrecy, and transparency requirements for online voting transactions are structurally very different from, and generally stricter than, those for E-Commerce transactions." The other major distinction is that "we can at least eventually detect E-Commerce errors and fraud, but we may never even know about online election fraud."[53] In other words, a consumer or banking customer will find out if unauthorized purchases are being made online with his or her credit card or if money is being drained out of a personal bank account.

However, a voter would probably never know that his or her vote was intercepted, changed, or otherwise manipulated before being cast on an Internet voting website or portal, because the necessary anonymity of the voting process makes it almost impossible to set up a verification system that also preserves ballot secrecy. Because of the requirements of the secret ballot, you cannot get a voting statement, like a banking statement, at the end of the month that tells you how election officials registered your vote the way you receive bank statements that list all of the specific transactions in your account.

Conclusion

While there is no doubt that being able to cast a ballot from your home computer, like being able to order and buy products and services through online Internet transactions, might make voting more convenient, the extraordinary security problems of such a remote Internet voting system present an extraordinary, unacceptable risk to election integrity. The overwhelming conclusion of computer experts is that those security vulnerabilities are inherent in the architecture and organization of the Internet and the software and hardware in common use today. Without major technological changes, there is almost no possibility that a secure Internet voting system can be designed for the foreseeable future. When combined with other less technical questions like equal access by voters to the Internet, Internet voting is definitely a technology whose time has not come—and may never come.

*—**Hans A. von Spakovsky** is Manager of the Election Law Reform Initiative and a Senior Legal Fellow in the Edwin Meese III Center for Legal and Judicial Studies at The Heritage Foundation. He is a former commissioner on the Federal Election Commission and counsel to the Assistant Attorney General for Civil Rights at the U.S. Department of Justice and the coauthor of* Who's Counting? How Fraudsters and Bureaucrats Put Your Vote at Risk *(Encounter, 2012) and* Obama's Enforcer: Eric Holder's Justice Department *(HarperCollins/Broadside, 2014).*

[52] Ibid.

[53] Ibid.