

RELEVANT DOCUMENTS, SOURCES AND QUOTES

U.S. Election Assistance Commission, Voting System Testing and Certification Division: A Survey of Internet Voting (9/11)

The U.S. Election Assistance Commission was established under the 2002 Help America Vote Act to help administer federal elections. "Internet security is a technical and policy issue that persists today. The questions raised more than a decade ago still pertain....(T)he current standard used to test voting systems at a federal level includes requirements for accessibility, security, and other voting-specific functionalities. This standard does not include requirements to test and certify Internet voting systems,....Currently a single comprehensive standard for developing and testing Internet voting systems does not exist."

<http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf>

National Institute of Standards and Technology, Information Technology Laboratory: Security Considerations for Remote Electronic UOCAVA Voting (2/11)

NIST was directed by the U.S. Election Assistance Commission to research remote voting technologies. UOCAVA stands for Uniformed and Overseas Citizens Absentee Voting Act. This report concluded that current internet voting systems are not as secure as in-person voting. "First, remote electronic absentee voting from personally-owned devices face a variety of potential attacks on voters and voters' personal computers. Since the voter's personal computer is outside the control of election officials, it is extremely difficult to protect against software attacks that could violate ballot secrecy or integrity of steal a voter's authentication credentials...Second, remote electronic voter authentication is a difficult problem. Current technology does offer solutions, but these may be difficult or expensive to deploy...Third, it is not clear that remote electronic absentee voting systems can offer a comparable level of auditability to polling place systems. (N)o current or proposed technologies offer a viable solution." Pg.59.

<http://www.nist.gov/itl/vote/upload/NISTIR-7700-feb2011.pdf>

CA Secretary of State: Report on the Feasibility of Internet Voting (1/00)

"(T)he public must be kept apprised of the manner by which the Internet is protected from outside influences, including national and international hackers as well as individual voters who might try to cast more than one ballot. Additionally, it is imperative that all voters are assured that their right to a secret ballot is protected and guarded jealously by government officials who themselves are kept aware of *who* has voted, but purposely are kept ignorant *how* individuals vote. This then is the fine line that those who administer Internet voting must walk --- audits must be possible, fraud must be impossible, and the secrecy of ballots must be ensured." Pg. 30.

http://www.sos.ca.gov/elections/ivote/final_report.htm#final-2

Computer Technologists' Statement on Internet Voting (9/11/08)

32 of the top professors, scientists, security experts and technologists signed a statement "Internet voting should only be adopted after these technical challenges have been overcome, and after extensive and fully informed public discussion of the technical and non-technical issues has established that the people of the U.S. are comfortable embracing this radically new form of voting."

www.verifiedvoting.org/downloads/Internet-voting-standards.pdf

Internet Voting in the U.S. (October 2012)

Communications of the ACM (the refereed flagship journal of ACM; ACM is the premier professional, scientific, and educational society for computing professionals)

Barbara Simons, Douglas W. Jones

The assertion that Internet voting is the wave of the future has become commonplace. We frequently are "If I can bank online, why can't I vote online?" is frequently asked. The question assumes that online banking is safe and secure. However, banks routinely and quietly replenish funds lost to online fraud in order to maintain public confidence. Many advocates also maintain that Internet voting will increase voter participation, save money, and is safe. The safety argument is surprising in light of frequent government warnings of cybersecurity threats and news of powerful government-developed viruses. The authors see little benefit in measures that may or may not improve voter turnout while casting doubt on the integrity of the results.

<http://cacm.acm.org/magazines/2012/10/155536-internet-voting-in-the-us/fulltext>

Issue Brief: Internet Voting and Uniformed and Overseas Citizens Absentee Voters (2010)

USACM (Association for Computing Machinery US Public Policy Committee)--the premier society for computer scientists, researchers, and educators.

As states provide electronic delivery of blank ballots, some are using the Internet for the return of voted ballots via email attachments. Vendors of online election software, with a vested interest in selling their products, of course downplay the inherent risks and promise "Internet security". But experts in computer security maintain that nothing sent over the Internet is secure. Voter's personal computers, from which emails are sent, are easily and constantly attacked by viruses, worms, Trojan Horses and spyware.

http://csrc.nist.gov/groups/ST/UOCAVA/2010/PositionPapers/EPSTEIN_InternetVotingUOCAVA.pdf

Broken Ballots: Will Your Vote Count? (2012) (Chapter 11: Voting Rights for Viruses?)

Douglas W. Jones, Barbara Simons

Published by the Center for the Study of Language and Information. Distributed by the University of Chicago Press.

The book begins with a comprehensive history of the use of technology in elections, starting with mechanical voting machines in the 19th century. Many of the problems that emerged then continue to plague modern electronic voting machines. The authors go on to illustrate how both legislation and the regulatory structure governing voting equipment have been ineffective at addressing technological risks – risks that frequently outstrip the understanding of election administrators and regulators. The result has been a series of failures where there is reason to doubt the official vote count correctly reflected the intent of the voters. Both Democrats and Republicans have been the victims of these failures. The book ends with a prescriptive summary that includes recommendations for policies and legislation to better protect the democratic process.

<http://www.brokenballots.com/>

Internet Voting, Security, and Privacy (2011)

Jeremy Epstein for the William and Mary Bill of Rights Journal, William and Mary School of Law.

"Internet voting is widely claimed to improve voter turnout and reduce costs. However there is no justification for either claim. Additionally, there are significant risks to voter disenfranchisement. Localities considering moving to Internet voting need to consider the technical factors.....Blank ballot distribution may be feasible, especially with dedicated systems, but other types of Internet voting are too risky to be used for public elections."

<http://scholarship.law.wm.edu/wmborj/vol19/iss4/4>

If I Can Bank Online, Why Can't I Vote Online? (updated 2011)

Jeremy Epstein, Stanford Research Institute International

"Potential problems with Internet voting fall into several categories, many of which are related to issues with voters' computers. Does the machine represent the voter's intent? ...Another set of issues crops up on the server side, where votes are collected."

http://www.computingreviews.com/hottopic/hottopic_essay_10.cfm

"My Vote is an I-Vote!": A detailed analysis about the possibility and limitations of internet voting (2011)

Ishwari Bendre, Theresa Juarez, Chris Li, Xida Zheng, Cal Tech

"Most damagingly, we believe that the benefits of internet voting are overstated, because they rely on a complete conversion to the technology. However, the most likely path to implementation is an incremental process that must take place alongside traditional voting technologies. Due to these issues, we think that internet voting will not be adopted in any meaningful form with the next decade."

<http://www.pickar.caltech.edu/e103/Final Exams/Internet Voting.pdf>

Evidence-Based Elections (May 2012)

P.B. Stark and D.A. Wagner, UC Berkeley, published in the IEEE Security and Privacy, Special Issue on Electronic Voting.

A short description of the problems with internet voting followed by a solution: evidence = auditability + auditing. "...elections should be structured to provide convincing affirmative evidence that the reported outcomes actually reflect how people voted. This can be accomplished with a combination of software-

independent voting systems, compliance audits, and risk-limiting audits.... compliance audits and risk-limiting audits should be required.”

<http://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf>

Internet Voting----Not Ready for Prime Time? (2/22/13)

Doug Kelleher, co-chair of New York’s State Board of Elections: “Right now, there is no way to meaningfully secure an election by Internet voting, and we’d be inviting serious potential for fraud on a scale that’s never been experienced in election administration before. Until methods can be designed to secure the election so that you know that every vote is being counted the way the voter cast it, I am opposed to Internet voting.”

<http://thevotingnews.com/internet-voting-not-ready-for-prime-time-the-canvass/>

Internet Voting: Will Democracy or Hackers Win? (2/16/12)

The West Virginia Secretary of State was interviewed about military voters faxing back their ballots thus losing anonymity. The director of the Pentagon’s Federal Assistance Program stated “I think it’s going to be five or six years before we’re even close to a point where we think that we could deploy a Department of Defense system in order to be able to meet or legislative mandate.”

http://www.pbs.org/newhour/bb/politics/jan-june12/internetvoting_02-16.html?print

Attacking the Washington, D.C. Internet Voting System (2/12)

Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, University of Michigan, Ann Arbor Washington D.C.’s pilot internet voting project was developed in 2010 for overseas absentee voters. Prior to launch, the District invited hackers to test the system. Within 48 hours of the system going live, University of Michigan students gained near-complete control of the election server, changed every vote, and revealed almost every secret ballot. The intrusion went undetected for 2 business days until the students instructed the program to play the University of Michigan fight song after voters completed their ballots. The students discuss how they did it and the “practical challenges of securing online voting as practiced today by a growing number of jurisdictions.”

<http://jhalderm.com/pub/papers/dcvoting-fc12.pdf>

Internet Voting option terminated by Edmonton CA City council (2/6/13)

http://www.edmonton.ca/city_government/municipal_elections/internet-voting.aspx

Online Voting ‘Premature,’ Warns Government Cybersecurity Expert (3/29/12)

Bruce McConnell, top cybersecurity official at the U.S. Department of Homeland Security. “It’s premature to deploy Internet voting in real elections at this time...when you connect (voting systems) to the Internet, that vulnerability increases.” Security around Internet voting is “immature and underresourced.”

<http://www.npr.org/blogs/itsallpolitics/2012/03/29149634764/online-voting-premature-warns-government-cybersecurity-expert>

APT1 Exposing One of China's Cyber Espionage Units (2/13)

Mandiant Corporation, a cybersecurity firm, released a study naming a Chinese People's Liberation Army unit as responsible for a long-running and extensive cyber espionage campaign against a broad range of victims since at least 2006. APT1 has compromised 141 companies spanning 20 industries, stealing large volumes of valuable intellectual property during repeated attacks.

http://www.intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Internet voting poses a risk (2/14/13)

David Jefferson, a Lawrence Livermore computer scientist, says that “hosting a national election online poses a national security threat.” He points to 3 fundamental areas of attack by hackers or viruses, with no immediate solutions for online voting: malicious software in a voter’s computer or smartphone, server side attacks, and denial of service attacks preventing people from voting.

<http://www.Dyn.politico.com/printstory.cfm?uuid=4A032D70-CB54-4FE2-B920-DFA8E053C690>

Internet voting for overseas military puts election security at risk (3/23/2013)

Pamela Smith of VerifiedVoting : “Just last week, we learned that the U.S. has already experienced our

first ever documented attack on an election system, when a grand jury report revealed that someone hacked into the Miami-Dade primary elections system in August 2012.” She goes on to recall a Washington Post report that Chinese hackers attacked most government entities in Washington, including the CIA, FBI, Department of Defense, and several financial institutions. “These organizations have huge cybersecurity budgets and the most robust security tools available, and they have been unable to prevent hacking. Contrary to popular belief, online voting systems would not be any more secure.”

<http://www.verifiedvoting.org/blog>

Electronic Voting and Electronic Counting of Votes (updated 12/2010)

The Australian Electoral Commission studied U.S. and Australian voting systems. “This paper does not suggest that Australian electoral authorities should at this stage embark on a program to fully replace the easily understood, publicly and politically accepted efficient, transparent paper ballot system that currently exists.”

<http://www.aec.gov.au/voting/report.htm>

Disadvantages of electronic voting (6/11)

Shama Obaed covers security problems of e-voting in Bangladesh. In addition to problems common to American systems, Bangladeshi e-machines could be corrupted by political ties between the ruling party and the manufacturers. The fear is manufacturers will tailor the e-voting machines to the ‘needs’ of the current political party in power.

<http://dailyalochona.blogspot.com/2011/06/alochona-disadvantages-of-electronic.html>

International Experience with E-voting: Norwegian E-vote Project (6/12)

Study of the issues and challenges related to internet voting: trust in Internet voting, secrecy and freedom of the vote, accessibility of Internet voting, and the role of stakeholders. “However, the implementation of Internet voting, according to emerging standards, is a very technical exercise. It can pose some difficult political questions if the aim is to facilitate the inclusion of large numbers of expatriate citizens in the political process.The need for secure online voter authentication mechanisms may be one of the biggest hurdles in implementing Internet voting.”

<http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~1>

Report on the Estonia Internet Voting System (2011)

Barbara Simons visited Estonia after their 2011 election in which 24% of the population voted over the internet. The results for the internet portion of the election differed significantly from the results from the paper ballot portion. Consequently, the leadership of the political party (the Center Party) that came in second believes that the internet portion was rigged. Since there is no way to recount an internet election, it was impossible either to convince them that the election was honest or to prove that it was rigged. The report discusses some of the security issues with internet voting in Estonia.

<http://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2>

Estonia gets to vote online. Why can't America? (11/6/12)

Online elections in Estonia work because everyone is issued a government ID with a scannable chip and a PIN number giving them a unique online identity. Votes are encrypted to preserve anonymity. There is less incentive for voter fraud because Estonia has a proportional representation government.

<http://www.washingtonpost.com/blogs/wp/2012/11/06/estonians-get-to-vote-online>

Think the Florida Recount was Bad? Just Wait Until November 6 (10/22/12)

Andrew Cohen of The Atlantic and 60 Minutes covers what has happened since the Help America Vote Act (HAVA) was enacted. New laws in the past 16 year to prevent voter fraud “has not created greater oversight over the security of electronic voting machines or the people who program and run them....Congress should amend the HAVA so that its oversight provisions are given teeth. Corporations which run our elections must be held more accountable.”

<http://www.theatlantic.com/politics/archive/2012/10/think-the-florida-recount-was-bad-just-wait-until-november-6/263901/>

Why You Can't Vote Online (11/5/12)

Ron Rivest of MIT said "I think when we talk about voting over the Internet, my gut reaction says: Why vote over the Internet? I think you need to ask that question a lot... There are other approaches to getting information back and forth that are better, and have better security properties. Voting over the Internet is rarely going to be the best choice. It's very complicated, and you are asking for trouble... You want something simple. You are entering a world of attacks and risk that you don't want to be in."

<http://www.technologyreview.com/news/506741/why-you-cant-vote-online/>

Recipe for Voter Fraud: Global Internet Voting Firm Buys U.S. Election Results Reporting Firm (1/15/12/)

Bev Harris of Black Box Voting reports the merger of SOE software company (which operates under the name ClarityElections.com) with SCYTL voting system based in Barcelona funded by international venture capital funds. "...there will be no ballots. No physical evidence. No chain of custody. No way for the public to authenticate who actually cast the votes, chain of custody, or the count."

<http://www.infowars.com/recipe-for-vote-fraud-global-internet-voting-firm-buys-u-s-election-results-reporting-firm/>

TED talk: I Can Bank Online. Why Can't I Vote Online? (November 5, 2012)

Barbara Simons

Many ask: Why can't I bank online but not vote online? Barbara Simons, co-authors of the book Broken Ballots, says neither is safe. Simons explains that no website is immune to outside attacks – not your bank's, not the CIA's and certainly not an online voting system developed by a locality for an election. In this talk, she gives a sobering truth: that the internet is fundamentally insecure and that online voting may never be a safe option.

<http://www.youtube.com/watch?v=Wv3VuGZzdK8>

Charlie Rose interview: Barbara Simons on her book "Broken Ballots: Will Your Vote Count? (October 4, 2012)

<http://www.charlierose.com/view/interview/12588>

Microsoft Research talk: Internet Voting; An Idea Whose Time Has Not Come (August 8, 2012)

There is now a widespread perception that Internet voting is the wave of the future and the way to save money while increasing voter participation, especially participation of young people. Not having learned from previous mistakes and against the advice of essentially all computer security experts, Internet voting is currently being used in several countries and in some U.S. States. There is also strong pressure to adopt Internet voting in the U.S. For members of the military and civilians living abroad. In this talk, Barbara Simons examines some of the threats of Internet voting in the hope of encouraging the technical community to oppose Internet voting unless and until these threats can be eliminated.

<http://research.microsoft.com/apps/video/dl.aspx?id=171182>