

## Internet Voting

Proposals to conduct voting pilots using real elections continue to reappear both in the U.S. and elsewhere, seemingly independent of warnings from computer security experts. While the appeal of Internet voting is obvious, the risks, unfortunately, are not, at least to many decision makers. While very few votes have ever been cast in American elections directly through a web interface, many states already allow military and overseas ballots to be returned via fax and email. Yet voted ballots sent via Internet simply cannot be made secure and make easy and inviting targets for attackers ranging from lone hackers to foreign governments seeking to undermine US elections.

### Further Reading

[ACM: Internet Voting in the United States](#)

[If I Can Shop and Bank Online, Why Can't I Vote Online?](#)

[What About Email and Fax?](#)

[Report on Internet Voting in Estonia](#)

[ACM Brief: Internet Voting and Uniformed and Overseas Citizens absentee Voters \(pdf\)](#)

Despite that, as states provide electronic delivery of blank ballots, some are using the Internet for 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 the oxymoronic "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.

Once a voted ballot is emailed, it 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.

There is no way to guarantee that the security, privacy, and transparency requirements for elections can all be met with any practical technology in the foreseeable future. Anyone from a disaffected misfit individual to a national intelligence agency can remotely attack an online election, modifying or filtering ballots in ways that are undetectable and uncorrectable, or just disrupting the election and creating havoc. There are a host of such attacks that can be used singly or in combination. In the cyber security world today almost all of the advantages are with attackers, and any of these attacks can result in the wrong persons being elected, or initiatives

wrongly passed or rejected. [Continue Reading](#)

## Computer Technologists Statement on Internet Voting

In 2008, Verified Voting founder David Dill organized the Computer Technologists' Statement on Internet Voting. The Technologist's Statement warns against "pilot" Internet voting projects and describes the severe challenges that must be met if an Internet voting system is to justify public confidence.

[Read The Computer Technologists' Statement on Internet Voting](#)

## Current Status of Internet Voting in the United States



Both e-mailing voted ballots and transmitting them through a Web portal are forms of “Internet voting.” And with the proliferation of Internet fax services, we can presume that many voted ballots returned to election officials via fax have in fact been transmitted through the Internet. Internet voting thus can mean voting from an Internet browser in one’s personal computer, or by email attachment, or electronic fax, remote kiosk, or other means of remote electronic transmission. A voted ballot sent through the Internet is no more verifiable than a polling place ballot cast on a paperless direct-recording electronic voting machine – and in fact is exposed to a far greater number of security threats including cyber-attacks such as modification in transit, denial of service, spoofing, automated vote buying, and viral attacks on voter PCs.

In all, 32 states allow military and overseas voters to return ballots electronically. Yet 22 of these states require that voting systems at home use paper ballots or provide voter-verifiable paper records. We cannot overstate this fact: the technological reasons that 35 States have moved toward paper ballots or voter-verifiable paper records for all voters at home and 10 more provide them for voters in at least some counties also apply, with even greater urgency, to voted ballots

returned to State and local election officials electronically from outside the country. Of the 32 States that allow electronic return of voted ballots, only New Jersey requires military and overseas voters to return a paper ballot in addition to sending their ballots to election officials in electronic form. This option provides verifiability, if the ballot of record for audits and recounts. Currently no State allows the transmission of voted ballots for stateside voters. You can view the specific provisions for the electronic submission of voted ballots in each of the States at the right of this page.

### **The Military and Overseas Voter Empowerment (MOVE) Act of 2009**

There's no question that voting for military and overseas voters needs to be improved. Too often absentee ballots are not received in time, if at all. Returning voted ballots from voters in hard to reach places (for example remote military outposts) in time to meet state election deadlines is difficult. These are real problems and 2009 saw efforts to improve ballot access for overseas voters kick-started by passage of the [Military and Overseas Voter Empowerment \(MOVE\) Act](#), passed as an amendment to the Defense Authorization bill. The MOVE Act addressed many problems facing overseas voters. It required that election officials provide ballots to military and overseas voters 45 days in advance of the election. Election officials must also make applications and blank ballots available electronically. Except for the issues raised by the remaking of ballots in some States, this is an excellent provision that allows technology to expedite the voting process but does not endanger the verifiability of the election. In addition, the MOVE Act established a system through which absent military voters are able to return their voted ballots by expedited mail through the U.S. Postal Service for free. But while the MOVE Act calls for electronic distribution of election materials, it is notably silent on the subject of return of voted ballots, with good reason.

Following enactment of MOVE, as states sought ways to meet new requirements for electronic delivery of ballots to voters deployed or living overseas, some states reached beyond the requirements of the Act. These states started providing electronic channels for return of voted ballots from voters: fax, email and Internet portals for uploading of voted ballots, and in some cases "online mark and send." The States are under *no* Federal requirement to permit electronic return of voted ballots, but many do so despite the major security risks. In addition, opportunity for error arises through the "remaking" of returned ballots, whether printed or electronic, onto optical scan ballots by election officials in order to insert the copies into the tabulating scanner. Ballots may be remade if the voter returns a printed and marked copy of an electronically received blank ballot, or if a completed ballot is returned electronically to election officials. In both cases the paper version of the "ballot" election officials receives or prints out currently cannot be scanned. There is little information about how widespread the practice of remaking electronically transmitted UOCAVA ballots is, and it may depend on how many UOCAVA voters vote in a given jurisdiction. [For more information and citations see Counting Votes 2012 \(PDF\)](#)

David Jefferson on Internet Voting:

Barbara Simons: Why can't we vote online?:

#### Internet Voting Reports

"Within 36 hours of the system going live, our team had found and exploited a vulnerability that gave us almost total control of the server software, including the ability to change votes and reveal voters' secret ballot." [Attacking the Washington, D.C. Internet Voting System](#) (2012)

"Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution." [Security Considerations for Remote Electronic UOCAVA Voting](#), NIST, February 2011

"The return of voted ballots poses threats that are more serious and challenging than the threats to delivery of blank ballots and registration and ballot request. In particular, election officials must be able to ascertain that an electronically-returned voted ballot has come from a registered voter and that it has not been changed in transit. Because of this and other security-related issues, the threats to the return of voted ballots by e-mail and web are difficult to overcome." [A Threat Analysis on UOCAVA Voting Systems](#), NIST December 2008

"Most of the security problems with Internet voting are generic to any PC and Internet application, and fundamentally have no effective solutions. This is why the majority of all email transmitted over the Internet is spam, and an estimated 50% of all Internet-connected PCs in the world are infected with malicious software, despite more than a decade of effort and immense investment by the world's high technology companies in trying to fix these problems. It is not just that no solution to the problems of Internet voting has yet been deployed. The real problem is that no fundamental solution is possible using the current Internet protocols and the current PC hardware and software platforms." [Comment on the May 2007 DoD report on Voting Technologies for UOCAVA Citizens](#), Aviel Rubin, David Jefferson, Barbara Simons, 2007

"The transmission of voting materials by unsecured email is a concern from both a privacy and security concern. Email traffic ... is easily monitored, blocked and subject to tampering. In addition, the publication of e-mail addresses of voting officials subject those offices to attack, effectively blocking voters." [Independent review final report for the Interim Voting Assistance System \(IVAS\)](#), Aug. 2006

"Because the danger of successful, large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE immediately and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear." [SERVE voting system security report](#), 2004

"Remote Internet voting systems pose significant risk to the integrity of the voting process, and should not be used for use in public elections until substantial technical and social science issues are addressed. The security risks associated with these systems are both numerous and pervasive, and, in many cases, cannot be resolved using even today's most sophisticated technology." [National Science Foundation Internet Voting Report](#), 2001

"[The] broad application of Internet voting in general faces several formidable social and

*technological challenges. ... They include providing adequate ballot secrecy and voter privacy safeguards to protect votes from unauthorized disclosure and to protect voters from coercion; providing adequate security measures to ensure that the voting system (including related data and resources) is adequately safeguarded against intentional intrusions and inadvertent errors that could disrupt system performance or compromise votes; providing equal access to all voters, including persons with disabilities, and making the technology easy to use; and ensuring that the technology is a cost-beneficial alternative to existing voting methods, in light of the high technology costs and security requirements, as well as the associated benefits to be derived from such investments."* [Elections: Perspectives on Activities and Challenges Across the Nation](#), GAO, October 2001

*"Our concerns about early and remote voting plans are even stronger as we contemplate the possibility of Internet voting. In addition to the more general objections, the Commission has heard persuasive testimony that Internet voting brings a fresh set of technical and security dangers all its own. This is an idea whose time most certainly has not yet come."* [National Commission on Federal Election Reform](#), Aug. 2001

*"Remote Internet voting poses serious security risks. It is much too easy for one individual to disrupt an entire election and commit large-scale fraud."*

[Voting: What is, what could be](#), Caltech-MIT Voting Technology Project, 2001

*"[T]echnological threats to the security, integrity and secrecy of Internet ballots are significant. The possibility of "Virus" and "Trojan Horse" software attacks on home and office computers used for voting is very real and, although they are preventable, could result in a number of problems ranging from a denial of service to the submission of electronically altered ballots."* [California Secretary of State's Task Force on Internet Voting](#) (2000)