

Speaking Against HB-5903

To the Honorable Co-Chairs Slossberg and Spallone and members of the committee:

My name is Michael Fischer. I am a resident and voter of Hamden, a professor of computer science at Yale, and a founding member and President of TrueVoteCT, a voter advocacy group dedicated to maintaining integrity of Connecticut elections. I appreciate the opportunity to address you this morning on House Bill 5903, which provides for the electronic transmittal of absentee ballots by military personnel.

Our troops who are fighting to defend our democracy certainly deserve our support in every way possible. However, compromising the election system that is at the heart of our democracy is hardly the way to give them that support. We expect our votes to be freely cast and to remain private. We depend on transparent voting systems to ensure that every vote is counted. We require voter verified paper ballots so that recounts are possible if anything goes wrong, and so that audits can be performed that give voters confidence in the integrity of the elections.

Unfortunately, non-polling place electronic voting is unable to meet these requirements for trustworthy elections. There is no way to ensure that voters are not coerced in their selections. Current technology is unable to guarantee ballot privacy on its long trip through the internet from military base to town official. The bill explicitly waives the requirement for a paper ballot, so there will be no way to perform a recount. Positively identifying the submitter of an electronic ballot also remains a difficult problem.

The Computer Technologist' Statement on Internet Voting, of which I am a signer, says:

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.

Connecticut isn't the first to suggest internet voting. The federally-funded SERVE program was abandoned in 2004 after security experts found that the online system could easily allow vote tampering. Last December, NIST issued a report on electronic technologies specifically in regard to the Uniformed and Overseas Citizens Absentee Voting Act. It says, "Voted ballot return remains a more difficult issue to address" and goes on to recommend only that "emerging trends and developments in this area should continue to be studied and monitored." NIST doesn't feel that the time is right to make the leap to electronic ballot submission, nor do I. HB5903 should be defeated.

I thank you for the opportunity to address you this morning. I would be pleased to answer any questions you may have.

Respectfully submitted,
Michael J. Fischer

80 Killdeer Road
Hamden, CT 06517
(203) 288-9599
fischer-michael@cs.yale.edu

Computer Technologists' Statement on Internet Voting

Election results must be *verifiably accurate* -- that is, auditable with a permanent, voter-verified record that is independent of hardware or software. Several serious, potentially insurmountable, technical challenges must be met if elections conducted by transmitting votes over the internet are to be verifiable. There are also many less technical questions about internet voting, including whether voters have equal access to internet technology and whether ballot secrecy can be adequately preserved.

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.

A partial list of technical challenges includes:

- **The voting system as a whole must be verifiably accurate in spite of the fact that client systems can never be guaranteed** to be free of malicious logic. Malicious software, firmware, or hardware could 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. Existing methods to "lock-down" systems have often been flawed; and even without that problem, there is no guaranteed method for preventing or detecting attacks by insiders such as the designers of the system.
- **There must be a satisfactory way to prevent large-scale or selective disruption** of vote transmission over the internet. Threats include "denial of service" attacks from networks of compromised computers (called "botnets"), causing messages to be mis-routed, and many other kinds of attacks, some of which are still being discovered. Such attacks could disrupt an entire election or selectively disenfranchise a segment of the voting population.
- **There must be strong mechanisms 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/or data.
- **There must be reliable, unforgeable, unchangeable voter-verified records** of votes that are at least as effective for auditing as paper ballots, without compromising ballot secrecy. Achieving such auditability with a secret ballot transmitted over the internet but without paper is an unsolved problem.
- **The entire system must be reliable and verifiable** even though internet-based attacks can be mounted by anyone, anywhere in the world. Potential attackers could include individual hackers, political parties, international criminal organizations, hostile foreign governments, or even terrorists. The current internet architecture makes such attacks difficult or impossible to trace back to their sources.

Given this list of problems, there is ample reason to be skeptical of internet voting proposals. Therefore, the principles of operation of any internet voting scheme should be publicly disclosed in sufficient detail so that anyone with the necessary qualifications and skills can verify that election results from that system can reasonably be trusted. Before these conditions are met, "pilot studies" of internet voting in government elections should be avoided, because the apparent "success" of such a study absolutely cannot show the absence of problems that, by their nature, may go undetected. Furthermore, potential attackers may choose only to attack full-scale elections, not pilot projects.

The internet has the potential to transform democracy in many ways, but permitting it to be used for public elections without assurance that the results are verifiably accurate is an extraordinary and unnecessary risk to democracy.

Endorsements

The computer technology experts below endorse this statement. Affiliations are for identification only, and do not imply that employers have a position on the statement.

Alex Aiken
Professor of Computer Science, Stanford University
<http://cs.stanford.edu/~aiken>

Andrew W. Appel
Professor of Computer Science, Princeton University
<http://www.cs.princeton.edu/~appel/>

David L. Dill
Professor of Computer Science, Stanford University and Founder of VerifiedVoting.org
<http://verify.stanford.edu/dill>

Jeremy Epstein
Software AG and Co-Founder, Verifiable Voting Coalition of Virginia
<http://www.visualcv.com/jepstein>

David J. Farber
Distinguished Career Professor of Computer Science and Public Policy Carnegie Mellon University
<http://www.epp.cmu.edu/httpdocs/people/bios/farber.html>

Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University
<http://www.cs.princeton.edu/~felten>

Michael J. Fischer
Professor of Computer Science, Yale University, and President, TrueVoteCT.org
<http://www.cs.yale.edu/people/fischer.html>

Joseph Lorenzo Hall
UC Berkeley School of Information
<http://josephhall.org/>

David Jefferson
Lawrence Livermore National Laboratory
<http://people.llnl.gov/jefferson6>

Bo Lipari
Retired Software Engineer, Executive Director New Yorkers for Verified Voting
<http://www.nyvv.org/bolipari.shtml>

Douglas W. Jones
Professor of Computer Science, University of Iowa
<http://www.cs.uiowa.edu/~jones/vita.html>

Robert Kibrick
Director of Scientific Computing, University of California Observatories / Lick Observatory
<http://www.ucolick.org/~kibrick>

Scott Klemmer
Assistant Professor of Computer Science, Stanford University
<http://hci.stanford.edu/srk/bio.html>

Peter Neumann
Principal Scientist, SRI International
<http://www.esl.sri.com/users/neumann>

Eric S. Roberts
Professor of Computer Science, Stanford University
<http://cs.stanford.edu/~eroberts/bio.html>

Avi Rubin
Professor, Computer Science, Johns Hopkins University
<http://avi-rubin.blogspot.com/>

Bruce Schneier
Chief Security Technology Officer, BT Global Services
<http://www.schneier.com/>

Yoav Shoham
Professor of Computer Science, Stanford University
<http://cs.stanford.edu/~shoham>

Barbara Simons
IBM Research (retired)
<http://www.verifiedvoting.org/article.php?id=2074>

Eugene H. Spafford
Professor and Executive Director of CERIAS, Purdue University
<http://spaf.cerias.purdue.edu/narrate.html>

Michael Walfish
Assistant Professor of Computer Science, University of Texas, Austin
<http://nms.csail.mit.edu/~mwalfish>

Dan S. Wallach
Associate Professor, Department of Computer Science, Rice University
<http://www.cs.rice.edu/~dwallach/>

Luther Weeks
Retired Software Engineer and Computer Scientist
http://www.ctvoterscount.org/?page_id=2

Jennifer Widom
Professor of Computer Science, Stanford University
<http://infolab.stanford.edu/~widom/>

Statement with questions and answers available at
<http://www.verifiedvotingfoundation.org/article.php?id=6611>