

S.B. 647 – Oppose as Unconstitutional, Risky, Unnecessary, and Discriminatory

**Veterans' Affairs Committee
Testimony – February 17, 2013**

**Luther Weeks
Luther@CTVotersCount.org
334 Hollister Way West, Glastonbury, CT 06033**

Chairs and members of the Committee, my name is Luther Weeks, Executive Director CTVotersCount, an experienced Certified Moderator, a Computer Scientist, and a Veteran.

I applaud this Committee for holding hearings on this Unconstitutional, Risky, Unnecessary, and Discriminatory bill. Last year, without hearings, this concept it was placed far down in an unrelated emergency bill.

Internet Voting Is Risky In Theory: The Computer Technologists Statement on Internet Voting details five technical challenges to such voting that have never been resolved and concludes: *“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.”*

Internet Voting Has Proven Risky In Practice: In September 2010, Washington D.C. opened their proposed internet voting system to ethical hackers. With very short notice, the system was compromised, changing all past and future votes. Separately, the municipal network was entered, passwords to municipal systems obtained, and the list of codes for Internet voting for all voters in the November election were obtained. Internet voting for the election was cancelled. Washington D.C. should be applauded for allowing the test, since most other jurisdictions have not subjected their systems to such testing. Just recently, a user compromised a test in Edmonton, Canada.
<http://tinyurl.com/CT2013sb283>

Email and Fax Voting Is More Risky Than Online Voting:

- Every week we hear of the compromise of email, databases, and servers maintained by large businesses and government agencies.
- We are all familiar with emails and faxes, we send or are sent to us, never being received. All network communications are subject to interception, substitution, or deletion. Military voters and registrars are not exempt from these problems.
- President Obama has called the protection of government and private information and communications networks *“one of the most serious ... security challenges of the 21st century,”* (Hartford Courant May 30, 2009.)

Registrars Are Not Equipped To Implement Email Or Fax Voting:

- Currently some towns do not provide Internet to their registrars and some do not provide email.
- Frequently, published email addresses for registrars are out of date.
- To whom would soldiers email votes? The Democratic or Republican Registrar? To a common email account? Who will process that? How can anyone be sure ballots that successfully arrive at an email account are not dropped or changed?
- Who manages the Fax? Who can see or discard the ballots that come via the Fax?

This Bill Is Unconstitutional: That is one of the reasons Governor Malloy vetoed last year's bill. The Connecticut Constitution says *“The right of secret voting shall be preserved.”* i.e. it is every voter's right that everyone's votes shall forever be anonymous. Anyone using the email account associated with such votes or handling a designated fax machine could see such votes.

This Bill Is Discriminatory: Many overseas voters are veterans but not members of the Military. Some serve in remote areas or challenging conditions. Including: State Department, CIA, and NGO staffs, plus Military Contractors, and Peace Corps volunteers.

This Bill Is Unnecessary: Conventional solutions for effective, safe, and economical Military voting are available and proven. The state with the best results for overseas voting, Minnesota, does not use online voting. Let's emulate their example.

Please join me, computer scientists, security experts, and advocates nationwide in opposing online and Internet voting in any form.

There is no need to applaud my military service. Yet, there will be every reason to applaud your service, if you drop this bill. It is an affront to the ideals for which all of our veterans and ancestors have given so much.

Thank you

Governor Malloy's 2012 veto message excerpt:

HB 5556 also contains a provision allowing deployed service members to return an absentee ballot by email or fax if the service member waives his or her constitutional right to a secret ballot. I agree with Secretary of the State Denise Merrill that this provision raises a number of serious concerns. First, as a matter of policy, **I do not support any mechanism of voting that would require an individual to waive his or her constitutional rights in order to cast a timely, secret ballot, even if such waiver is voluntary.** Second, as the Secretary of the State has pointed out, **allowing an individual to email or fax an absentee ballot has not been proven to be secure. In 2011, the United States Department of Commerce, National Institute of Standards and Technology, issued a report on remote electronic voting. The report concluded that remote electronic voting is fraught with problems associated with software bugs and potential attacks through malicious software, difficulties with voter authentication, and lack of protocol for ballot accountability.** None of these issues are addressed in this bill. To be clear, I am not opposed to the use of technology to make the voting process easier and more accessible to our citizens. However, I believe that these legitimate problems have to be carefully studied and considered before enacting such a provision.

NPR video of a representative of the Department of Homeland Security discussing why the Internet is not safe for voting:

<http://ctvoterscount.org/dhs-expert-internet-voting-not-secure/>

The state with the best record of serving Military and all Overseas voters does not employ Internet, email, or fax voting. That state is Minnesota. It has an exemplary record of implementing the MOVE Act, with the assistance of the Overseas Vote Foundation (OVF). Here is Minnesota Secretary of State, Mark Ritchie's talk from Jan 24, 2013 at the OVF forum for more information. See the OVF for more information on how Military and Overseas voters would like to be served:

Video: <http://tinyurl.com/b7cxu78> OVF: <https://www.overseasvotefoundation.org/>

View the video of the Secretary of the State Denise Merrill's *Symposium On Online Voting*, held for the benefit of the General Assembly, with Nationally recognized experts on Internet voting:

<http://ctvoterscount.org/secretary-of-the-states-online-voting-symposium/>

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, leak information about votes to enable voter coercion, prevent or discourage voting, or perform online electioneering. Existing methods to "lock-down" systems have often been flawed; even if perfect, 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.

<http://www.verifiedvotingfoundation.org/article.php?id=6611>

Endorsements [Computer Technologists' Statement on Internet Voting]

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

Andrew W. Appel
Professor of Computer Science, Princeton University

Ben Bederson
Associate Professor, Computer Science Department,
University of Maryland

L. Jean Camp
Associate Professor, School of Informatics, Indiana
University

David L. Dill
Professor of Computer Science, Stanford University and
Founder of VerifiedVoting.org

Jeremy Epstein
Software AG and Co-Founder, Verifiable Voting Coalition of
Virginia

David J. Farber
Distinguished Career Professor of Computer Science and
Public Policy Carnegie Mellon University

Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton
University

Michael J. Fischer
Professor of Computer Science, Yale University, and
President, TrueVoteCT.org

Don Gotterbarn
Director, Software Engineering Ethics Research Institute,
Computer and Information Sciences, East Tennessee State
University

Joseph Lorenzo Hall
UC Berkeley School of Information

Harry Hochheiser
Assistant Professor, Computer and Information Sciences,
Towson University

Jim Horning
Chief Scientist, SPARTA, Inc., Information Systems Security
Operation

David Jefferson
Lawrence Livermore National Laboratory

Bo Lipari
Retired Software Engineer, Executive Director New Yorkers
for Verified Voting

Douglas W. Jones
Professor of Computer Science, University of Iowa

Robert Kibrick
Director of Scientific Computing, University of California
Observatories / Lick Observatory

Scott Klemmer
Assistant Professor of Computer Science, Stanford
University

Vincent J. Lipsio

Peter Neumann
Principal Scientist, SRI International

Eric S. Roberts
Professor of Computer Science, Stanford University

Avi Rubin
Professor, Computer Science, Johns Hopkins University

Bruce Schneier
Chief Security Technology Officer, BT Global Services

John Sebes
Co-Director, Open Source Digital Voting Foundation
Chief Technology Officer, TrustTheVote Project

Yoav Shoham
Professor of Computer Science, Stanford University

Barbara Simons
IBM Research (retired)

Eugene H. Spafford
Professor and Executive Director of CERIAS, Purdue
University

Michael Walfish
Assistant Professor of Computer Science, University of
Texas, Austin

Dan S. Wallach
Associate Professor, Department of Computer Science, Rice
University

Luther Weeks
Retired Software Engineer and Computer Scientist

Jennifer Widom
Professor of Computer Science, Stanford University

David S. Wise
Computer Science Dept., Indiana University