

Comments—NBP Public Notice #20.

GN Docket Nos. 09-47, 09-51, and 09-137

Verified Voting Foundation <http://verifiedvotingfoundation.org> appreciates the opportunity to comment on NBP Public Notice #20, GN Docket Nos. 09-47, 09-51 and 09-137. Our non-partisan, nonprofit organization promotes accessible, reliable, publicly verifiable elections in the US. Please find below our responses to the questions posed.

Pamela Smith, President

Voting. Voting is the most fundamental of civic acts. As technology transforms all aspects of society, could voting be transformed as well?

a. With existing technology, is it possible to enable and ensure safe and secure voting online today?

In a word, no. For details, please see <http://verifiedvoting.org/internet> and <http://www.verifiedvotingfoundation.org/article.php?id=6734>

The Computer Technologists' Statement on Internet Voting, whose signatories include some of the world's principal authorities on computer security, states the challenges of Internet voting eloquently:

“Multiple studies by computer scientists have shown that making Internet voting safe is an incredibly hard problem, not solved yet, and possibly unsolvable. According to technology expert and former chair of the Association of Computing Machinery (ACM) Barbara Simons, “If ballots are cast on the Internet, attacks on the election can be made by anyone with an Internet connection anywhere in the world, including individual hackers, political parties, international criminal organizations, hostile foreign governments, or even terrorists.”

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.”

To inspire confidence and demonstrate reliability, a voting system must include a way for voters to know – i.e. on a hard copy – that their votes were recorded as they intended, and for election officials to subsequently prove that those votes were counted accurately. In other words, there must be a mechanism independent of the voting system’s software by which that software’s functioning can be checked, and by which election results can be recovered if computer technology fails.

In banking systems, the ability to connect a record with a customer and the thorough paper trail makes this kind of auditing possible. In voting systems, the need to prevent connecting a vote with the voter who cast it makes this extremely difficult, unless there is a voter-verified paper ballot which is used in post-election audits to check the system for accuracy.

b. What can we learn from other nations that have considered or implemented online voting?

Other nations’ experiences are substantively different because of the very complex nature of US elections by comparison. Significant problems have been reported in online voting systems in other nations, however. The most critical factors are the absence of any auditability in these online voting systems, and issues relating to privacy and vote-secrecy.

A system in the Netherlands was scrapped after researchers found numerous problems with the code which would render it insecure. This was one of the largest internet voting systems worldwide and it employed cryptographic end to end verification systems. They named "fundamental problems with vote secrecy" as part of the reason for the decision.

From a report in Finland, The Supreme Administrative Court ruled on the Finnish municipal elections of October 2008, in which an Internet voting system was piloted. In its decision, the court sided with the complainants, overturning an earlier decision of Helsinki Administrative Court, and the decisions of the municipal central elections committees to confirm the election results. As a result, the three municipalities that took part in the Finnish e-voting pilot were required to hold new elections as soon as possible. The new elections would use a traditional paper ballot system.

c. What can we learn from pilot projects that have tested online voting?

Pilot projects are not a reliable measure for testing online voting. There is no predictability of security from a pilot to a real election. Anyone who wished to use the vulnerabilities of the system to tamper with an election, or compromise the privacy of the voters, would almost certainly not do so during a pilot. This does not mean they *could* not tamper, only that they *likely would* not tamper during the pilot. The signatories of the Computer Technologists' Statement on Internet Voting have recommended against “pilot studies” for this reason (please see comment on item f).

d. Have localities or states enabled online voting either domestically or for citizens abroad (such as military personnel stationed overseas)?

Some states are plunging into allowing electronic return of voted ballots for overseas voters, with little or no examination of the technological risks involved. In recent years, jurisdictions defended the “security” of paperless electronic voting systems in polling places by saying “our systems cannot be hacked – they are never connected to the Internet at any time.” Yet some jurisdictions are moving to casting of ballots through online transmission. Other jurisdictions, such as the states of Michigan and Ohio, are progressing with significantly more (well-deserved) caution and prohibiting the return of ballots online or permitting only the transmittal of blank ballots to overseas voters online, but not the return of voted ballots.

Recent interest in online voting is ironic in light of the ongoing discussion over the security of electronic voting systems. For much of this decade, reassurance about the security of polling-place e-voting systems has included the contention that the systems are secure “because they are never connected to the Internet.” Indeed, a number of states including Mississippi, New York, California, Ohio, and Texas, have enacted laws or issued standards that prohibit any connection of polling-place voting devices and county election servers to the Internet. How prototype Internet voting systems differ so from current electronic voting systems that they obviate such wise security provisions has never been adequately explained.

Overseas and military voters face significant challenges being able to vote in the available time frame from when ballots and materials are available and the deadline for returning those ballots. The Pew Center on the States wrote a report called “No Time To Vote” which explains this in detail. As they point out in the report, these challenges can be resolved WITHOUT having to resort to insecure voting practices such as returning voted ballots electronically. At no point in this report is online voting recommended as a solution to these problems. See http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Election_reform/NTTV_Report_Web.pdf

e. Do government jurisdictions at any level, domestic or foreign, allow online voting for any citizen? Have there been quantifiable impacts tied to online voting, including impacts on the number of citizens that voted? Have there been qualitative impacts tied to online voting, either positive or negative?

In Hawaii, a local (community, non-governmental) election carried out earlier this year using online voting resulted in a near 80% decrease in turnout compared to the previous election cycle. Voters who did not have access to the Internet were permitted to vote by phone, but this did not appear to help increase turnout.

f. What are the security and privacy risks that government jurisdictions must consider when considering the implementation of online 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 above list of challenges and text derive from the Technologists’ Statement on Internet Voting, found at <http://verifiedvoting.org/Internet> . The signatories include:

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/>

Ben Bederson
Associate Professor, Computer Science Department,
University of Maryland
<http://www.cs.umd.edu/~bederson>

L. Jean Camp
Assoc. Professor, School of Informatics, Indiana
Univ.
<http://www.ljean.com/>

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>

Don Gotterbarn
Director, Software Engineering Ethics Research
Institute, Computer and Information Sciences, East
Tennessee State University
<http://csciwww.etsu.edu/gotterbarn>

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

Harry Hochheiser
Assistant Professor, Computer and Information
Sciences, Towson University
<http://triton.towson.edu/~hhochhei>

Jim Horning
Chief Scientist, SPARTA, Inc., Information Systems
Security Operation
<http://www.horning.net/pro-home.html>

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
Asst. Professor of Computer Science, Stanford Univ.
<http://hci.stanford.edu/srk/bio.html>

Vincent J. Lipsio
<http://www.lipsio.com/~vince/resume.pdf>

Peter Neumann
Principal Scientist, SRI International
<http://www.csl.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 Univ.
<http://avi-rubin.blogspot.com/>

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

John Sebes
Co-Director, Open Source Digital Voting Foundation
Chief Technology Officer, TrustTheVote Project
<http://www.osdv.org/who>

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
Prof. and Exec. Director of CERIAS, Purdue Univ.

<http://spaf.cerias.purdue.edu/narrate.html>

Michael Walfish
Assistant Professor of Computer Science, Univ. 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/>

David S. Wise
Computer Science Dept., Indiana University
<http://www.cs.indiana.edu/~dswise/>

g. What are the history and current state of play of online voting technologies?

Private vendors in the US and also based overseas are actively pushing these technologies because there is profit to be made. These considerations cannot outweigh the security and reliability – and auditability – of US elections under any circumstances. There have been several internet primaries in the last few years, including a primary conducted by Democrats Abroad in 2008. In many cases, these schemes have been deployed without due consideration of the technical challenges, based on unsupported assertions by vendors that the systems are "secure".

When a Department of Defense proposal for internet voting in the 2004 presidential election was reviewed by computer security experts, it was terminated because of [security concerns documented by those experts](#). *The \$22 million Internet voting system for troops — Secure Electronic Registration and Voting Experiment (SERVE) — was scrapped "because we didn't have confidence in the security of it," Maj. Burr said.* [Source:

<http://washingtontimes.com/news/2004/may/23/20040523-112919-6616r/>] While it is true that technology has advanced since that date, the consensus among technical experts continues to be that today's Internet is not ready for online voting, and may not be for a very long time to come.

h. What are best practice processes concerning online voting?

A respected technologist well-versed in election technology from the Massachusetts Institute of Technology said that “developing best practices for Internet voting is a lot like developing best practices for drunk driving. In either case, you just don’t want to go there.”

The best practice is to use online technologies to provide INFORMATION and BLANK BALLOTS to voters overseas. Such technology should NOT be used for returning/casting voted ballots.

We believe there is a need for in-depth, public debate on the technical and NON-TECHNICAL issues in internet voting before adopting it. It's very possible that a technically sound internet voting scheme could be rejected for non-technical reasons, including other issues such as whether internet voting might disenfranchise legal voters who cannot easily access the internet.

i. How would enabling online voting impact overseas military personnel, overseas diplomatic personnel or other Americans living overseas?

Military and other overseas citizens face significant challenges to be able to participate in elections. Verified Voting supports improvements that will better the ability for our men and women in uniform and other overseas citizens to be able to cast effective ballots, and we participate in an alliance of organizations <http://amovr.org> working to examine ways in which those improvements can be promulgated. We believe that overseas voters can be better served by providing them with an auditable voting system that uses online technologies only for delivery of information and as needed for delivery of blank ballots to them.

A 2008 report by the National Institutes of Standards and Technology (NIST) [<http://vote.nist.gov/uocava-threatanalysis-final.pdf>] makes this point, and does not endorse online return of voted ballots:

"Fax, e-mail and Web-based systems could distribute blank ballots quickly and reliably to voters, significantly reducing the ballot delivery times faced by mailing ballots to voters and improving the ... voting experience for citizens overseas," the report says. "In addition, registration and ballot requests can also take advantage of these distribution methods, but there are more threats when handling personal information from voters. Voted ballot return remains a more difficult issue to address." (Source: <http://www.itworld.com/government/59789/nist-finds-security-problems-overseas-e-voting>)

While some might see enabling online voting as a convenience, closer examination of the real technical challenges to being able to do so securely makes it clear that the cost of such a convenience is greatly outweighed by the risks. The problems facing overseas voters, though real and considerable, *can—and must--* be solved through other means.