

Comments on proposals to allow Internet, email, and fax voting in Washington State Barbara Simons

We must do everything in our power to ensure that our military serving overseas have the opportunity to vote, and that their votes are correctly counted. As MOVE provides, electronic transmission of information and materials is appropriate. However, MOVE does not require electronic transmission of voted ballots. Rather, MOVE calls for “expedited mail delivery service” via the U.S. Postal Service.

I enthusiastically support the first part of Section 1 of HB 2483 and SB 6238: “An overseas or service voter may receive a ballot by fax, e-mail, or other electronic means.” I also strongly recommend that you to delete the following sentence: “An overseas or service voter may return a voted ballot by fax or e-mail if the voter's signature on the declaration accompanies the ballot”.

And I urge you to defeat internet voting bills HB 1624 and SB 5522.

Cybersecurity is a growing concern – with ever more frequent reports of government and corporate sites getting hacked, as illustrated by a recent major Internet-based attack on Google originating from China. That attack targeted Gmail accounts of Chinese human rights activists. Furthermore, according to the Wall Street Journal, as many as 34 companies were attacked, including Yahoo, Adobe, and Juniper Networks. It appears that even Symantec and Northrop Grumman were targeted.

Not only do the companies named by the Wall Street Journal have vastly more resources than the relatively small Internet voting vendors, but they also employ large numbers of computer security experts. In fact, Symantec's major products include anti-virus and anti-spyware software.

Another way in which hackers, criminals, or foreign countries could manipulate Internet-based elections is by inserting election-rigging software into voters' computers. The easiest way to do this is by distributing a virus or worm over the Internet. The Conficker worm, which infected between 9 and 15 million machines in November 2008, can even “call home” for updates.

Anti-virus software works by checking for known viruses and worms. Therefore, whenever a new virus appears, the anti-virus software must be updated. There can many days between the time when the virus is initially distributed and when it is recognized and analyzed. After that, the virus fix needs to be distributed, and users need to disinfect their machines – at times a very difficult step.

While many viruses and worms are planted without the knowledge of the computer owner, people are sometimes willing to download software of highly questionable provenance. In August 2009 a spam message circulate that said, “If You dont like Obama come here, you can help to ddos his site with your installs.”[sic] (ddos stands for Distributed Denial of Service, an attack that overwhelms a website, making it inaccessible). According to CNET News, people who clicked on the email link were offered money in exchange for downloading denial of service software. They were even told to return to the website for updated versions if their virus detection software deleted the original download. The source of the spam is not known. The goal could be to disrupt websites associated with Obama, to engage in identity theft, or even to infect machines of Obama opponents, something that could be especially useful if Internet voting were to become an option in the United States.

Once a voter's computer is infected by a virus or worm, all bets are off. The virus can make the computer screen show the voter a ballot image that correctly represents the voter's intent. But the virus

can then send something entirely different over the Internet. In other words, ***it is the virus that is voting, not the voter***. The voter will never know, because it is impossible for the voter to see what is actually sent.

All email, which uses the Internet, is subject to the insecurities of the Internet. Because it is extremely difficult to encrypt email and because email and fax transmissions are routed through the phone systems of the country of origin, there are additional security issues for voters living or stationed abroad. Anyone intercepting the email or fax can make arbitrary changes to the ballot, or even prevent the ballot from being delivered. It is not possible for the Department of Defense to guarantee the security of telecommunications outside the U.S., especially when electronic communications might be routed through unfriendly countries.

Furthermore, both fax ballots and email ballots (it's trivial to change the header of an email) would be easy to forge.

In many ways, Cyberspace is today's lawless wild west. We must honor our military and overseas voters by ensuring that we have established strong cybersecurity criteria before we even think about experimenting with their voted ballots transmitted through cyberspace.

By providing military and overseas voters with blank ballots via the Internet, you will cut the time required to vote in half. If there is still a problem, there are secure solutions, such as mailing the voted ballots back via Fed Ex.

Voting is the cornerstone of our democracy, and an insecure voting system is a national security threat. We must not make the votes of our servicemen and servicewomen vulnerable to hackers from China or elsewhere – people who might have the ability to determine the next Governor of Washington State, or perhaps even the next President of the United States.

Barbara Simons

An expert on electronic voting, Dr. Barbara Simons is on the Board of Advisors of the U.S. Election Assistance Commission. She was a member of the National Workshop on Internet Voting that was convened at the request of President Clinton and produced a report on Internet Voting in 2001. She also participated on the Security Peer Review Group for the US Department of Defense's Internet voting project (SERVE) and co-authored the report that led to the cancellation of SERVE because of security concerns. Simons co-chaired the Association for Computing Machinery (ACM) study of statewide databases of registered voters. She recently co-authored the League of Women Voters report on election auditing. Simons and Doug Jones are co-authoring a book on voting machines.

Simons was President of ACM, the nation's oldest and largest educational and scientific society for computing professionals, from July 1998 until June 2000. She founded ACM's US Public Policy Committee (USACM) in 1993 and served for many years as the Chair or co-Chair of USACM.

In 2005 Simons became the first woman to receive the Distinguished Engineering Alumni Award from the College of Engineering of U.C. Berkeley. She is also a Fellow of ACM and the American Association for the Advancement of Science. She received the Alumnus of the Year Award from the Berkeley Computer Science Department, the Distinguished Service Award from Computing Research Association, the Making a Difference Award from ACM's Special Interest Group on Computing and Society, the Norbert Wiener Award from Computer Professionals for Social Responsibility, the Outstanding Contribution Award from ACM, and the Pioneer Award from the Electronic Frontier Foundation. She was selected by C|NET as one of its 26 Internet "Visionaries" and by Open Computing as one of the "Top 100 Women in Computing." Science Magazine featured her in a special edition on women in science.

Simons served on the President's Export Council's Subcommittee on Encryption and on the Information Technology-Sector of the President's Council on the Year 2000 Conversion. She is on the Board of Directors of VerifiedVoting.org. She has also been on the boards of the U. C. Berkeley Engineering Fund, the Electronic Privacy Information Center, Public Knowledge, and the Oxford Internet Institute, as well as the Advisory Council of the Public Interest Registry's ORG. She has testified before both the U.S. and state legislatures and at government sponsored hearings. She was runner-up in the first election for the North America seat on the ICANN Board.

Simons co-founded the Reentry Program for Women and Minorities in the Computer Science Department at U.C. Berkeley. She is also on the Boards of the Coalition to Diversify Computing (CDC) and the Berkeley Foundation for Opportunities in Information Technology (BFOIT), groups that work at increasing participation in computer science of women and underrepresented minorities.

Simons earned her Ph.D. in computer science from the University of California, Berkeley. Her dissertation solved a major open problem in scheduling theory. In 1980, she became a Research Staff Member at IBM's San Jose Research Center (now Almaden). In 1992, she joined IBM's Applications Development Technology Institute as a Senior Programmer and subsequently served as Senior Technology Advisor for IBM Global Services. Her main areas of research have been compiler optimization, algorithm analysis and design, and scheduling theory. Her work on clock synchronization won an IBM Research Division Award. She holds several patents and has authored or co-authored a book and numerous technical papers. She is retired from IBM Research.