The Honorable Charles Schumer
Chairman, Committee on Rules and Administration
United States Senate
305 Russell Senate Office Building
Washington, DC 20510

May 19, 2009

Re: Senate Hearing on Problems for Military and Overseas Voters
Wednesday May 13,2009, 10:00am

Dear Chairman Schumer,

Thank you for ensuring that the problems that military and overseas voters have in participating in the democratic process – and knowing their votes are counted – is not forgotten with the end of the 2008 federal election cycle. And thank you especially for looking for solutions to this very serious problem.

Everyone Counts was founded with the mission of ensuring Universal Access to a full ballot for all citizens entitled to vote, and additionally ensuring that each submitted ballot is securely delivered and reliably counted. Our work has provided secure and accessible voting channels for voters in the UK, Australian military voters serving alongside our own military in Iraq and Afghanistan, Democrats living abroad, and most recently, voters in Honolulu Hawaii in federal, state and local elections throughout the past decade. We ensure that voters have the ability to vote privately, securely and independently, and that those ballots are reliably counted – no matter where the voter is on Election Day.

And we would be honored to help election officials in the US learn how to provide those same benefits for UOCAVA voters from the US. Attached you will find our whitepaper comparing the various methods – mail, email, fax and secure Internet and telephone voting – for serving UOCAVA voters, as well as our whitepaper demonstrating the successful results of providing secure and accessible online voting for the Australian military serving in Iraq and Afghanistan for their federal Parliamentary election in 2007 and Democrats Abroad for the US Presidential primary in 2008.

As I write this, Everyone Counts and the City and County of Honolulu are demonstrating the ability to provide these same secure voting channels to voters on US soil. The world's first completely digital Universal Access election opened on May 6 and will run through May 22, offering secure online and telephone voting for a local Honolulu election. This is a model for increasing access and security for voters, while saving costs for governments.

Senator, thank you for taking steps to ensure that the long-term and serious challenge that US voters living or serving overseas face comes to a stop. We would be delighted to provide you with greater detail on the success we have had in serving overseas voters, as well as any other questions you may have.

Sincerely,

Lori J. Steele
Chief Executive Officer,
Everyone Counts, Inc.
lori@everyonecounts.com

Secure Remote Voting for Overseas and Disabled Voters

by Aaron Contorer

Chief of Products and Partnerships

Everyone Counts, Inc.

May 2009

Election officials are now taking online electronic voting seriously. Computer and phone networks can be useful channels for remote voters including soldiers and civilians overseas (UOCAVA), disabled (HAVA), and others.

Are computers and phones more or less secure than paper? What about fax? Can email be relied upon? How about the web or the Internet itself?

In this paper we explore what can and cannot be done with online voting technologies.

Reliable and timely access to a blank ballot

As a recent report from the National Institute of Standards and Technology (NIST) explained, the easiest-to-solve portion of UOCAVA voting is simply delivering ballots to voters. Technologies as simple as email and fax can transmit a blank ballot quickly anywhere in the world.

However, *a ballot which cannot be successfully voted and returned and counted is no better than no ballot at all*. Thus, the rest of this paper explores the rest of the problem.

Safe and reliable return of ballots

As the NIST report said, "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 email and Web are difficult to overcome."

Do you bank online? And is any money still in your account? Despite unlimited motivation to break into these systems, criminals are unable to penetrate online banking systems and drain the money. So we know that Internet services purpose-built for security can work well.

Does your bank let you withdraw money by email? Banks know that email is not secure. By the mid 1990s computer experts knew that in mere seconds an email can be made to appear "from" any person and any organization, regardless of its true origin. Better email software has been invented, but the system most Internet users use today is no more secure than it was in 1990. Furthermore, most email systems provide no privacy from the eyes of the sender's computer system administrator. Until we replace or reconfigure voters' email software worldwide, email is clearly not the answer to returning secret ballots securely.

Would you send a legal document by fax? You certainly can, and it works, and it's legal. Would you send a *secret* legal document by fax? Only if you are a very trusting individual. Voting rights advocates are furious about cases where citizens are required to vote by fax: this often involves completely sacrificing their right to a secret ballot. Faxes can be read on a phone line, and they often sit in plain sight at the receiving station. Making an altering or invalidating mark on a faxed ballot requires only a pen. And far from anonymous, faxes are automatically marked with their location of origin (whether accurate or faked). Fax is a handy technology, but utterly unsuitable for the return of secret ballots.

How does the military convey critical, time-sensitive, secret information? The answer is *digital encryption.* Extremely complicated mathematical formulas scramble the message with long numeric passwords or *keys,* yielding a series of numbers that read as nonsense to anyone lacking the secret decoding passwords.

Our company currently uses a military-grade system with an ever-changing 168-digit binary key, to encrypt each completed ballot before sending it to the tabulation office. Computers pick a new secret key for each ballot. Even a spy using a giant supercomputer could not hope to decode a single boxful of these ballots.

Encryption protects privacy but also prevents alteration: any change to the stream of numbers results in only gibberish when decoded.

Preventing invalidation

As we work to protect the rights of overseas and disabled voters, preventing the accidental invalidation of their ballots is crucial. We have all seen overseas military personnel going to great effort to vote, only to find their ballots discarded due to extraneous marks, overvoting, or the failure to fill out a signature block in the required format. Voters with disabilities have sent in many ballots whose intents were clear, but that were invalidated due to technical mistakes or extraneous marks.

Fax doesn't help, nor does email – even paper and a postage stamp do nothing to prevent accidental invalidation. Online voting, with real-time error checking before final submission, helps protect voters' right to be counted.

Assistive devices

Many blind, motor-impaired, or otherwise disabled persons have a computer or telephone which has been adapted to suit their needs. Online voting, by working with these adaptive devices, allows disabled voters to vote from home without the loss of privacy implied by manual assistance.

The secure audit trail

Auditors must ensure the proper custody and treatment of each ballot, from the moment it was cast until the count is complete.

The most auditable systems are the fully-online systems, in which each ballot can be tagged with an anonymous tracking number if desired.

The least auditable system is email. The Internet's system for routing emails was never designed to be auditable, and it is impossible to verify the path taken by an ordinary email between the sender's PC and the receiving machine. The email may go through any number of "server" computers in between – and as most are totally unencrypted, any server has the power to change or add to the contents. It is *routine* for servers to add to or alter emails, such as by adding routing information or noting whether the content looks suspicious. Many even discard emails without notice, as a defense from spam. Today's worldwide email infrastructure can be neither trusted nor audited.

Similarly, faxes may be electronically relayed and may be edited by the relayer manually or automatically. This is only common in large organizations, which use "e-fax" rather than "direct-dial fax" systems. The final receiver has no way to determine the number of relays or

edits a fax has been through, due to the lack of encryption.

Preventing "mystery software"

Mechanical balloting and mechanical tabulation introduced the "black box" problem: what is really happening inside that machine? Tests are routinely administered to detect defects and fraud attempts, yet tales of machine-assisted election tampering go back many years.

While even the simplest voting machine is subject to tampering, doubts grow dramatically when the machine contains parts – such as secret software – that election officials are *not allowed to see.* Computer experts agree this constitutes a serious risk – we must know what the machine is doing with the ballots, that they are being recorded and tabulated accurately and honestly.

The solution is *open code.* The technical workings of any device that handles votes should be fully open for inspection by officials. Software that is available to inspect is called *open code.* Open doesn't imply "free to copy" – seeing my blueprints doesn't license you to build my device. Many software experts believe that any voting computer should – or must – use open code.

Proof of receipt

Computers can effortlessly index vast amounts of information. Secure tabulation computers can let voters look up their ballots long after election day is over. Days after the election, a voter can visit a web site, enter his or her receipt number, and see a secret word or phrase he chose as proof that his ballot arrived safely.

This feature is one example of the power of technology to increase voter access and trust to levels impossible with paper ballots. In coming years we will see more such innovations throughout the voting systems industry.

Immunity from tampering

A well-designed trusted service can use other less-trusted technologies without danger. For example, paper ballots can be delivered using ordinary mail, not special "voter mail," because the security is provided by special envelopes, ballot boxes, and careful handling procedures. Similarly, online voting systems can use ordinary Internet technologies to move information around the globe, as long as the voting systems add proper security to what's already there.

The Internet equivalent of an envelope is encryption. When a message is encrypted, just like a paper inside a safety envelope, it cannot be read or altered along the way. Voting software using military-grade encryption can safely deliver ballots across any kind of Internet connection with no risk of spying or tampering. The better the voting software, the safer the ballot, regardless of how poor the voter's Internet connection may be.

What about *paper?*

None of us would demonstrably and routinely *obstruct* participation in elections. Yet that is just what voting by paper does, especially when the voter is overseas.

The Australian Electoral Commission state that when they provided the option for overseas soldiers to vote online, the number who were able to vote on time and be counted rose from 22 percent to 75 percent. And as reported in the *National Journal,* when the US Democratic

Party allowed expatriates in the recent Presidential primary to vote abroad, voter registration increased tenfold, and 54% chose to vote online (vs. only 3% for paper mail and fax combined).

Many completed ballots arrive late or never, and many will be invalidated – and the great majority will never exist at all, because soldiers and other expats are simply too busy to deal with balloting by mail.

Paper gets a failing grade for ease of access (wait for it to come in the mail), security (a dishonest postal official can read or even alter your ballot), reliability (foreign postal services are notorious for delaying and losing mail), and access for the blind and motor-impaired. There is no encryption of the contents, nor timely verification of delivery.

If paper were not a familiar old technology, we would never seriously propose using it today. While we all like paper, its obviousness and its tangibility, modern online technology is more secure, accessible, timely, reliable, and usable.

Continuity of Service

One of the risks with any technology is that it will break. This gets worse when someone is motivated to break it on purpose.

Polling stations are subject to any number of obstructionist techniques. However illegal, we all know that these happen. Similarly, those with criminal intent may interfere with the mail. And absentee ballots can be mishandled by relatives or volunteers claiming to help.

Electronic technologies are not immune from these sorts of shenanigans. Malicious individuals seeking to interfere with an election can attempt to jam up phone lines, fax lines, or Internet connections, or to somehow cause a malfunction of the receiving phone system, fax system, or computer system.

Fortunately technologists have many years of experience protecting technical infrastructure from such threats. Large corporations routinely receive threats from criminals hoping to extort money from them; yet the web sites continue to run, telephones continue to be answered, merchandise continues to be shipped, and bank accounts continue to reflect the deposits made.

Every election technology will always be subject to malicious behavior from the enemies of democracy, or from sore losers who don't expect to win the day's election. We must be ever vigilant against such attacks. Technology does not make human nature better or worse, but it does provide us with tools and well-tested techniques for security.

Protecting voters from misdirection

Lately we have heard about fake or incorrect registration information sent to voters in the mail. The citizen who thinks he has registered but has not, or who thinks he has cast a ballot but has not, has effectively been cut out of the election.

Every channel has some "point of entry" where the voter shows up ready to vote, and must not be fooled by cheaters. While it is hard to secretly build a fake polling place, or to somehow answer a voting phone number that you don't own, it is relatively easy to print a fake paper absentee ballot.

Somewhere in between these two is the difficulty of building a fake web site. Fortunately there are techniques for a website to prove its authenticity. These can be as simple as telling

each voter a personal secret number which the website must present, or as sophisticated as using an encrypted digital signature to prove the website's identity.

Overall we should consider telephone voting the hardest nut to crack for would-be fake pollsters; computer voting is also challenging; and paper voting is probably the easiest. Since we currently use paper for almost all absentee voting, this problem will get better through the use of technology.

Conclusions

Remote and disabled citizens must have their constitutionally mandated right to vote. Today's solution, paper, is failing miserably on timeliness, usability, and reliability – and it shows in the low numbers of military and overseas citizens who get their votes counted, and the great dissatisfaction of disabled advocacy groups. Technology can be used to solve many or even all of these problems – but it must be the right technology. Email is a totally unacceptable solution, and fax has numerous limitations. Online (computer and phone) systems have the most potential to serve remote and disabled users, as seen in use by banks and the military, when designed and used correctly to deliver on their security promises.

☐☐☑

About the Author

Aaron Contorer is Chief of Products and Partnerships at Everyone Counts, Inc., which provides accessible, transparent, and verifiably secure multi-channel election services.

Mr. Contorer is a former executive of Microsoft, where he served as Bill Gates' technology advisor, and as architect for the transition of MSN onto the Internet. He is an inventor on over a dozen patents in computer security and networking.

See summary table on next page.

Appendix: Technical Approaches to UOCAVA Access

Scale: None – Poor – Fair – Good – Excellent

Requirement	***Paper***	***Email***	***Fax***	***Online Phone***	***Online PC***
Deliver Blank Ballot	Slow	Fast	Fast	Instant	Instant
Prevent Invalidation	None	None to Fair	None	Excellent	Excellent
Privacy	Good (if not disabled)	Poor - Fair	Poor	Good - Excellent	Excellent
Prevent Alteration	Fair	Poor	Poor to Fair	Excellent	Excellent
Access for Blind	None - Poor	Good	None - Poor	Excellent	Good
Access for Motor Impaired	Poor	Good	Poor	Excellent	Good
Audit	Good - Excellent	Poor	Poor to Good	Excellent	Excellent
Evidence of Receipt	None	Fair	Good	Excellent	Excellent
Black Box Solved	Excellent	Poor	Good	Excellent	Excellent
Prevent Denial of Service	Good	Good	Good	Good	Good
Prevent Misdirection	Poor	Fair	Fair	Good	Good

Proven Innovation Solves Problems Surrounding Military & Overseas Voters' Ability to Fully Participation in Elections

By Paul DeGregorio

What if only one in six eligible Americans attempted to vote in a general election? And then what if only one-third of those who attempted actually had their ballots cast or counted? Why didn't the other 83% even try? How can an election be fair when nearly 95% of voters are unable to participate and have their votes counted?[i]

This is currently the case for America's military and overseas voters.[ii]

But the USA is not alone in this regard. Nearly 250 million people throughout the world reside outside of their regular electoral constituencies.[iii] And over 100 countries require their election officials to serve these remote voters while they are outside the country.[iv]

Increasingly, many officials are recognizing that the continued use of 100-year old voting methods won't work to solve these issues.[v]

In countries outside of the United States, tried, tested, and transparent online voting channels are now bringing the reach of democracy to the millions of overseas and disabled voters who have until now, been unable to participate.

Online voting is now accepted for a wide range of high integrity private elections such as shareholder votes and labor union ballots, with demand increasing each year. Use in binding public elections, which have typically been subject to controlled pilots, is also increasing worldwide.[vi]

The earliest pilot to serve military voters was deployed by the U.S. Department of Defense in 2000 in a very limited trial. Since then, pilots have continued throughout the world: Intensive government pilots of online voting have run for more than 8 years in the UK, an ex-patriot voting system has been deployed in the Netherlands, online local voting is ongoing in Switzerland and Canada, and in 2007 the national election in Estonia included an online voting channel for all voters, including disabled voters, and in Australia, military voters serving in Iraq and Afghanistan were able to vote via the Internet in a hotly-contested national Parliamentary election. In addition, political parties in the USA, UK and Canada have been utilizing online voting to increase participation of their members since 2000.

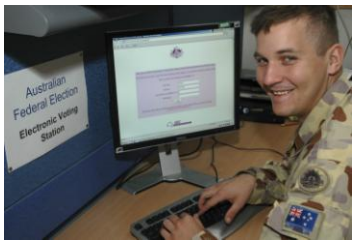
The U.S. remains behind, with only one attempt at implementation since the success of 2000. In 2004 the Secure Electronic Registration and Voting Experiment (SERVE) sought to provide true remote Internet voting for military serving abroad. However, the contracted system was questioned close to the deployment date in 2004 and the system shelved.[vii]

Some of those questions involved the security of online voting. In fact, while some electronic voting devices and traditional ballot boxes can be attractive targets for fraud, given that each collects hundreds of votes, a remote voter's PC is a far less attractive target for fraud. One remote PC is likely to collect only one or two votes. Further, an attacker has no way of accurately knowing which PCs will be used for remote voting.

Online voting applications can benefit voters by increasing accuracy. Computer-based voting can prevent over-votes and minimize under-votes and also can use multiple languages and even pictures and audio to assist with illiteracy.[viii] Unlike many current systems, however, remote online voting also provides for very strong receipting.

This paper highlights two case studies that demonstrate how proven channels of voting are being used abroad to decrease barriers and increase participation of the groups most disenfranchised by current voting systems.

Australia: Increasing Access for Military Voters



Australia is a parliamentary democracy whose elections are often called just 30 days or so before polling day. This makes it difficult—if not impossible—for ballots to be mailed to voters overseas and even more difficult for their ballots to be returned in time to be counted. Because of this, while voting is compulsory for most Australians, it is not for military personnel.

To verify the magnitude of the problem, a study was completed after the 2004 Federal Election by the Australian Electoral Commission (AEC). The study showed a problem similar to that in the United States: postal ballots were received for the election from only 22.8% of military personnel deployed overseas to operational areas.

Recognizing the seriousness of such a high disenfranchisement rate, the AEC brought the issue to the attention of the Australian parliament, who took decisive action to rectify the problem. They set a plan in motion to ensure that when the next parliamentary election was called, the AEC would be ready to enfranchise their military voters through secured online voting.

And ready they were.[ix]

In 2006, the AEC established a project that would involve a partnership between its office, military representatives in the Department of Defense, and Everyone Counts, Inc., a company with extensive experience in providing secure innovative solutions utilizing online and telephone voting systems.[x]

The system provided by Everyone Counts had to meet stringent audit requirements before it could be used and installed on a specially purposed array of servers within the DoD that would be controlled by the Australian Electoral Commission. A test lab contracted by the AEC performed an independent deep audit of the source code. It was required to prove that the source code was resistant to any malicious tampering, presented an accurate representation of votes cast in the printed record and was unable to allow the association of a voter with the vote cast.

In addition, the AEC observed builds of the software and any changes to the code that were requested. Access to the voting servers was highly restricted.

Cryptography and encryption ensured votes remained secret and protected. Voter authentication took place via the server (not the voting applet) using a technique where non-identifying credentials form the basis of uniqueness and sparseness and identifying credentials (such as DOB, SSN or similar) were strongly hashed by the applet. All votes were authenticated at least twice. To increase security and prevent the potential for internal security breaches, decryption took place on an off-line system using a private key that was protected by a thresholding system.

The net result of this very successful online voting pilot was a system that increased military voter participation in the November 2007 parliamentary election four-fold. Not a single vote was challenged or contested. The system was universally praised by voters and election officials.

Increasing Access for US Voters Abroad in 2008

Democrats Abroad (DA) is an official body of the U.S. Democratic National Committee, representing thousands of U.S. voters affiliated with the Democratic Party. Clearly aware of the difficulty that Americans living abroad have in obtaining and returning a ballot in time to be counted in U.S. elections, Democrats Abroad researched options to facilitate participation in the DA presidential primary scheduled for February 2008. Observing that online voting had been utilized successfully by political parties in other countries, they announced the first-ever multi-channel “Global” primary election.

Democrats Abroad offered their members the ability to vote in one of four ways. Once registered with DA, overseas Democrats could choose to vote in person at one of 100 designated caucus sites located 30 countries; receive and mail a ballot to their DA country representative; receive and send their ballot by fax; or cast their ballot online. Internet voting was offered through a secured system developed by Everyone Counts, Inc.

DA designated the period of February 5-12, 2008 for the balloting, with a deadline of January 31 for voters to join and sign up at their website, www.votefromabroad.com. Once registration closed, a voting list was developed and qualified voters were sent authentication and voting information. The Internet voting mechanism was web-based and utilized a secure server that was continually monitored for attacks (none occurred). The voting applet gave voters the opportunity to vote for any one of the Democratic Party candidates. The system allowed for voters to print a copy of their voted ballot and also have their online ballot cancelled before close of voting if they received and voted an absentee ballot from their home state (they were asked to vote in either one or the other).

Adding an online voting channel resulted in a seven-fold increase in participation, with military and civilian Americans casting their online ballots from 164 countries, including Antarctica. Voters chose voting by Internet more than 2 to 1 over voting in person, by mail and by fax, combined!

Like the Australian military voting project, the first-ever Democrats Abroad online Global Presidential Primary was a tremendous success. Many voters who have been disenfranchised before were able to vote.

These case studies, along with successful Internet voting projects elsewhere, prove that the time is now for policymakers and election officials to offer more – not fewer - opportunities for voters to have their voices heard – and have their votes counted.

Paul DeGregorio is the former Chairman of the U.S. Election Assistance Commission (EAC), COO of IFES-Democracy at Large and Director of Elections in St. Louis County, Missouri USA. He is currently COO of Everyone Counts, Inc (www.everyonecounts.com) and can be reached at paul@everyonecounts.com

[i] See EAC UOCAVA Report on 2006 election; Tables 21c and 22. http://www.eac.gov/News/docs/uocava-report-final-4-printing.pdf/attachment_download/file

[ii] See " Sam Wright: Another Election Decided by Disenfranchised Military Personnel" http://www.military.com/Opinions/0,,Wright_122704,00.html

[iii]See Jeremy Grace: *Challenging the Norms and Standards of Election Administration*: External and Absentee Voting (IFES, 2007), p. 35-58

[iv] International Institute for Democracy and Electoral Assistance (International IDEA) www.coe.int/.../democracy/EVoting/IDEA%20-%20Gratschew%20-%20ExV%20Strasbourg%20November%202006.ppt

[v] See "Military Voting and the Law: Procedural and Technological Solutions to the Ballot Transit Problem" found at: www.vote.caltech.edu/media/documents/wps/vtp_wp53.pdf and Medill Reports: "Military voting riddled with complications, inconsistencies" 3/08.

http://news.medill.northwestern.edu/washington/news.aspx?id=80819 and "Despite Laws, Disabled Voters Face Barriers at Polls" 10/06

http://newstandardnews.net/content/index.cfm/items/3822

[vi] See "Online Voting Clicks in Estonia" Wired, 3/07 www.wired.com/politics/security/news/2007/03/72846?currentPage=all

[vii] See ""*Point, Click, and Vote: the Future of Internet Voting,"* R. Michael Alvarez and Thad E. Hall. Brookings Institution Press. 2004. Washington, DC. http://www.brookings.edu/press/Books/2004/pointclickandvote.aspx

[viii] See"*Electronic Elections: The Perils and Promises of Digital Democracy"* by R. Michael Alvarez & Thad E. Hall; Princeton University Press 2008.

[ix] See: Remote Overseas Voting for Australian Defence Force Personnel

http://www.aec.gov.au/Voting/e_voting/adf.htm

[x]See http://www.everyonecounts.com/index.php/news/34/37

Submitted to the National Association of Secretaries of State (NASS) for their White Paper Series. July 2008