COMMON CAUSE
Holding Power Accountable

Verifiedvoting
Foundation.org

Statement on the Dangers of Internet Voting in Public Elections

At a time when more and more transactions occur online, a number of election officials and private organizations are looking to the Internet as one more possible avenue for balloting. When the Academy of Motion Picture Arts and Sciences announced that would be using an online voting system to help its members choose this year's Oscar nominees and finalists, thereby adding to the "credibility" of online voting, we find ourselves compelled to remind the general public that it is dangerous to deploy voting by email, efax, or through Internet portals in public governmental elections at this time. Public elections run by municipal, local and state governments should not be compared to elections like the one run by the Academy. The following describes our concerns about the use of Internet voting systems in public elections.

- Cyber security experts at the National Institute of Standards and Technology[1] and the Department of Homeland Security[2] have warned that current Internet voting technologies should not be deployed in public elections. Internet voting systems, including email, fax and web based voting systems in which marked ballots are cast online, cannot be properly protected and may be subject to undetectable alteration.

- Citizens ask, "If I can bank online, why can't I vote online?" Online banking and e-commerce are NOT secure, despite massive business investments in state-of-the-art cyber-security tools.

- Banking policies protect and reimburse people whose money or credit card numbers are stolen online. If a hacker deletes or alters a ballot, the action can neither be traced nor corrected.

- Banking policies generally do not protect companies when funds are stolen from their accounts. It has been reported that as many as ten percent of small business have had money stolen from their bank accounts.[3] Even so, businesses understand and accept that money lost through cyber-crime is part of the risk of doing business online, and they seek to reduce losses by obtaining fraud insurance. We cannot take that approach in counting votes in public elections; a cyber-attack that alters or deletes just a few hundred votes, and perhaps even fewer, can change the result of an election. There is no such thing as "fraud insurance" for ballots, and we can scarcely accept online fraud in ten percent of our election jurisdictions.

[1] http://www.nist.gov/itl/vote/uocava.cfm

[2] http://www.npr.org/blogs/itsallpolitics/2012/03/29/149634764/online-voting-premature-warns-governmentcybersecurity-expert

[3] http://www.nytimes.com/2012/06/14/business/smallbusiness/protecting-business-accounts-from-hackers.html?pagewanted=all&_r=0

- The parties in online business transactions maintain and audit account records to detect fraudulent activities. But because we vote by secret ballot in public elections, individual voters have no way to check and verify that their ballots were properly counted. Thus online voting is particularly susceptible to tampering, all but certain to go undetected.

- Internet voting system vendors make claims about the security of their products that have never been substantiated by publicly reviewable testing and research.

Ron Rivest, a well-known security expert from Massachusetts Institute of Technology, a co-founder of RSA Security, and recipient of the prestigious Turing Award[4], is an outspoken critic of Internet voting. "Vendors may come and they may say they've solved the Internet voting problem for you, but I think that, by and large, they are misleading you, and misleading themselves as well," Rivest told a Princeton University symposium last fall. "If they've really solved the Internet security and cyber security problem, what are they doing implementing voting systems? They should be working with the Department of Defense or financial industry."[5]

We conclude that the evidence does not exist to support casting ballots online in public elections. There are too many unsolved security challenges that have yet to be overcome. In fact securing networks from cyber attack is a major national security concern that is as yet unresolved. Financial institutions, the FBI, the White House, the Department of Defense have all been breached. Major corporations like Lockheed Martin, Sony, Google, Adobe, Microsoft, and Northrop Grumman have also been breached. It is unreasonable to assume that any Internet voting system vendor today can repel a well funded partisan operative or nation state determined to manipulate, disrupt, or violate voter privacy in an online public election.

Dr. David Dill, Professor of Computer Science, Stanford University

Bob Edgar, President, Common Cause

Jeremy Epstein, Senior Computer Scientist, SRI International

Dr. David Jefferson, Computer Scientist, Lawrence Livermore Laboratory

Dr. Justin Moore, Computer Scientist, Google

Dr. Peter Neumann, Principal Scientist, SRI International Computer Science Lab, Moderator, ACM Risks Forum

Dr. Ronald L. Rivest, Viterbi Professor of Computer Science, MIT

Dr. John A. Savage, An Wang Professor of Computer Science, Brown University

Dr. Barbara Simons, IBM Research (retired), Former President, Association for Computing Machinery (ACM)

Pamela Smith, President, Verified Voting

Dr. Philip B. Stark, Professor and Chair, Department of Statistics, University of California, Berkeley

Detailed bios of the signatories can be found here

[4] http://amturing.acm.org/

[5] http://www.technologyreview.com/news/506741/why-you-cant-vote-online/

February 14, 2013