The Viability of Responsible Internet Voting

Remote voting[[1]](#footnote-1) entails significant risks above and beyond those of in-person poll-site voting. Included among these are risks to integrity – as remotely-cast ballots may pass through numerous hands without independent observation – and risks to privacy – as voting takes place without the benefit of publicly-enforced voter isolation.

Internet voting substantially exacerbates the risks of remote voting by making it possible for small problems to be magnified and replicated on a large scale. Careless or malicious errors, intrusive malware, and unforeseen omissions – all of which can be caused by individuals or very small groups – can cause very large numbers of votes to be changed and the privacy of large numbers of voters to be compromised.

The technology known as end-to-end (E2E) verifiability allows individual voters to verify that their intended votes have been properly recorded and that all recorded votes have been properly counted. When applied to in-person voting, E2E-verifiability provides new assurances to voters by allowing them to check for themselves that the results of an election are correct. When applied to Internet voting, E2E-verifiability mitigates some of the risks described above – but does not eliminate them: voters are able to check that their ballots are properly recorded and counted, but malware can still compromise privacy, prevent voters from casting their ballots, and otherwise hinder voters.

Although E2E-verifiable election technologies have existed for more than thirty years, their use has thus far been limited to small demonstration systems and private elections for student governments, professional societies, and the like. E2E-verifiable elections produce new challenges and complications for implementers and administrators. They represent a new and different paradigm for elections – substantially replacing the notion of verification of election equipment with that of verification of the integrity of individual elections. As such, it is important to act deliberately and gain experience with E2E-verifiability in more manageable environments before attempting to deploy E2E-verifiable elections in their most challenging environment: the Internet.

These realities lead us to two principal conclusions.

1. **Public elections should not be conducted over the Internet using systems that are not end-to-end verifiable.**
2. **End-to-end verifiable Internet voting systems should not be used before end-to-end verifiable poll-site voting systems have been widely-deployed and experience has been gained from their use.**

The second of these two principles is also necessitated by the fact that an E2E-verifiable election must have a tally to verify, and if an E2E-verifiable system is used only for remote voters, then the votes of these remote voters must be separately tallied and reported. Few jurisdictions are willing to segregate and report the tallies of local and remote voters separately.[[2]](#footnote-2)

We take no position here as to whether the integrity benefits of E2E-verifiability and the privacy benefits it makes possible outweigh the risks of remotely-executed large-scale corruption of an Internet-based election, but we are agreed upon the conclusions that “naked” Internet voting is dangerous and irresponsible and that E2E-verifiability should be deployed in the less risky and more manageable scenario of in-person poll-site voting before it is deployed in the wilds of the Internet.

1. Remote voting is defined here as voting without the benefit of the public monitoring that takes place in a traditional poll site. [↑](#footnote-ref-1)
2. Note that if an E2E-verifiable system were deployed for poll-site voters only, ballots from remote voters could be incorporated into the system without full E2E-verifiability for remotely-cast ballots. A hybrid system of this kind would enjoy all of the protections of current systems and then some. Ultimately, it may be possible to provide remote voters with E2E-verifiable functionality as well and create a unified system that is fully end-to-end verifiable for all voters. [↑](#footnote-ref-2)