Testimony of Professor Ronald L. Rivest (MIT) about
internet voting (aka electronic ballot return),
to the Vermont State Legislature.

May 2023

Thank you for allowing me to provide testimony on a proposal to allow ``online ballot return'' (also sometimes known as internet voting).

I'd like to begin by introducing myself. Who am I?

My name is Ron Rivest, and I'm an Institute Professor at the Massachusetts Institute of Technology, in the department of Electrical Engineering and Computer Science. I've been at MIT since 1974. The opinions expressed here are my own.

I'm a co-inventor of the RSA encryption method that uses the product of two large prime numbers. This method has been standardized and is in widespread use today. I founded the companies RSA and Verisign based on this technology.

I'm a founding member of the CalTech / MIT Voting Technology Project.

I was a member of the Technical Guidelines Development Committee, advisory to the U.S. Election Assistance Commission; there I chaired the Security and Privacy subcommittee.

I am member of both the National Academy of Engineering and the National Academy of Science. I was recently a member of their committee on ``Securing the Vote: Protecting American Democracy.''

Most recently, I was a member of the Berkeley Public Policy Working Group on Internet Ballot Return, which is directly relevant to today's topic.

What is my testimony?

In short, I do not believe that the technology exists to make online ballot return adequately secure. A proposal along these lines should be rejected, in spite of it being well-motivated.

This is not just my opinion; I believe it is the consensus of security experts.

The 2018 report of the National Academy committee on ``Securing the Vote'' recommended that

> ``At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots.''

More recently, the 2022 statement by the Berkeley Public Policy Working Group on Internet Ballot Return, said

> ``The Working Group concludes that the current cybersecurity environment and state of technology make it infeasible for the Working Group to draft responsible standards to support the use of internet ballot return in U.S. public elections at this time.''

Basically: Online Ballot Return is not ready for prime time.

Informally, putting a server online to support online ballot return is like asking a kid to go play in traffic. It just isn't safe.

The proposal does not say anything about coping with malware on the voter's machine--an unsolved problem. The voter's machine may tell the voter that it has cast a ballot for the voter, when in fact it has done nothing, or worse, done the opposite.

The proposal does not explain how voters can verify that their ballots are cast as they intended. This is also an unsolved problem (one that is solved with voter-verified paper ballots).

The proposal does not explain how to cope with distributed denial of service attacks, where the new portal is overwhelmed with spurious requests and shut down. This is also an unsolved problem.

Finally, the proposal may leave election officials very unhappy, as they may have to answer questions of the form, ``Why did my candidate lose?'' with the sad refrain, ``I don't know, but the portal says your candidate lost.'' There is no sensible audit or recount possible with online ballot return.

To summarize, I urge you to vote against any proposal for ``electronic ballot return'' (or ``internet voting''). We just aren't ready for online ballot return.

Thank you for your attention.

Links:

NASEM Report: Securing The Vote: Protecting American Democracy
https://nap.nationalacademies.org/catalog/25120/securing-the-vote-protecting-american-democracy

Berkeley Working Group on Internet Ballot Return:
https://gspp.berkeley.edu/assets/uploads/page/Working_Group_Statement_on_Internet_Ballot_Return_.pdf

Website of Professor Ronald L. Rivest
http://people.csail.mit.edu/rivest/