Why experts are overwhelmingly skeptical of online voting

Aurich Lawson / Getty Images

reader comments

120 with 68 posters participating, including story author

Share this story

If anyone was going to be enthusiastic about online voting, it would be Ben Adida. After starting multiple dot-com startups in the late 1990s and early 2000s, Adida earned a computer science PhD from MIT in 2006. Studying under legendary cryptographer Ron Rivest (the “R” in RSA) at MIT, Adida explored how to use advanced cryptography to hold provably secure elections.

Adida created open-source online voting software called Helios based on that research. And more recently, he founded VotingWorks, a non-profit organization that creates open-source software for ballot-marking machines and post-election auditing.

“If I felt like Internet voting was viable, I would be really well-positioned to do it,” Adida told Ars in a recent phone interview. “I did my PhD on it. I run Helios as a side project.”

But Adida told us that online systems like Helios are “great for student elections, not for public elections.”

“Every couple of months I get someone who says can we use Helios for a public election,” Adida said. “I say, ‘You really shouldn’t.'”

That theme was echoed by other election security experts I talked to in recent weeks. Take David Becker, the executive director of the Center for Election Innovation and Research. He’s generally an advocate for the use of digital technology in elections. For example, he’s a staunch supporter of the controversial touchscreen ballot-marking devices used in Georgia elections. But like Adida, he argues we’re nowhere close to having technology to securely cast votes on the Internet. “I’ve not seen any evidence that we can do so verifiably, securely, and auditably,” Becker told Ars last month.

In 2018, West Virginia experimented with allowing 144 overseas service members to vote online using an app called Voatz. And this February, West Virginia passed legislation to expand online voting to disabled voters. The state was widely expected to again use Voatz for this, but West Virginia switched to software called OmniBallot for the June 2020 primary. It’s not clear what voting technologies West Virginia will use in November’s election.

Voatz CEO Nimit Sawhney has an ambitious vision for the future of American democracy. In two hour-long interviews with Ars—one in June, the other this week—he argued that everyone should have the option to cast votes online. He’s frustrated by widespread skepticism about online voting among election security experts like Adida and Becker.

Enlarge / A look at the Voatz app interface (Android version)
“How can you claim it’s settled science that Internet voting can never be safe?” he asked in a June interview. “Three hundred years ago we knew the Earth was flat and the Sun was revolving.”

Few of the experts I talked to said online voting could never be safe. But almost all of the independent experts I interviewed said it would be many years—if not decades—before it was feasible to build a secure voting system online.

Voatz is far from the only company working on online voting—other online voting systems have gotten equally harsh reviews from security experts. In June, we covered research by MIT computer scientist Michael Specter and the University of Michigan’s Alex Halderman that analyzed OmniBallot.

“We find that OmniBallot uses a simplistic approach to

Internet voting that is vulnerable to vote manipulation by malware on the voter's device and by insiders or other attackers who can compromise Democracy Live, Amazon, Google, or Cloudflare," the researchers wrote. "Using OmniBallot for electronic ballot return represents a severe risk to election security and could allow attackers to alter election results without detection."

MIT researchers found serious flaws

Voatz offers what seems like a simplified voting solution. Registered voters start with a smartphone app available for both iOS and Android. Votes are transmitted to servers hosted on Amazon Web Services and a copy is stored to a blockchain. The blockchain supposedly offers extra security by making it harder to tamper with votes later.

Last year, after it has already been utilized in a state election system, researchers from MIT undertook one of the first in-depth, independent reviews of Voatz software. "We find that Voatz has vulnerabilities that allow different kinds of adversaries to alter, stop, or expose a user's vote," the researchers wrote in February.

The researchers didn't have access to Voatz servers, so they focused their analysis on Voatz's mobile app. One of their big findings was that Voatz's protections against on-device malware were ineffective. The Voatz app comes with software called Zimperium that scans a smartphone for known malware and prevents the app from running if it is detected. But the MIT researchers demonstrated that it was possible to modify the Voatz app to prevent Zimperium from running in the first place.

Once these security checks are disabled, the Voatz app can be modified to undetectably change voters' choices. "It is straightforward to modify the app so that it submits any attacker-desired vote, yet presents the same UI as if the app

recorded the user’s submitted vote,” the researchers wrote.

The MIT study got a scathing response from Voatz. The company complained that the researchers had studied an outdated version of the Android app. And without access to the real Voatz servers, Voatz wrote, the researchers “fabricated an imagined version of the Voatz servers, hypothesized how they worked, and then made assumptions about the interactions between the system components that are simply false.”

https://arstechnica.com/?p=1699485