Online voting is a danger to democracy, says computer scientist

June 8 2016, by Ian Chipman

If, like a growing number of people, you're willing to trust the internet to safeguard your finances, shepherd your love life, and maybe even steer your car, being able to cast your vote online might seem like a logical, perhaps overdue, step. No more taking time out of your workday to travel to a polling place only to stand in a long line. Instead, as easily as hailing a ride, you could pull out your phone, cast your vote, and go along with your day. Sounds great, right?

Absolutely not, says Stanford computer science professor David Dill. In fact, online voting is such a dangerous idea that computer scientists and security experts are nearly unanimous in opposition to it.

Dill first got involved in the debate around electronic voting in 2003, when he organized a group of computer scientists to voice concerns over the risks associated with the touchscreen voting machines that many districts considered implementing after the 2000 election. Since then, paperless touchscreen voting machines have all but died out, partly as a result of public awareness campaigns by the Verified Voting Foundation, which Dill founded to help safeguard local, state, and federal elections. But a new front has opened around the prospect of internet voting, as evidenced by recent ballot initiatives proposed in California and other efforts to push toward online voting. Here, Dill discusses the risks of internet voting, the challenge of educating an increasingly tech-comfortable public, and why paper is still the best way to cast a vote.

Why should we be so wary about introducing computers, and in particular the internet, into the voting process?

Computers are very complicated things and there's no way with any reasonable amount of resources that you can guarantee that the software and hardware are bug-free and that they haven't been maliciously attacked. The problems are growing in complexity faster than the methods to keep up with them. From that perspective, looking at a system that relies on the perfectibility of computers is a really bad idea.

Compared with touchscreen voting machines, the opportunity for attacks on the internet is much broader. Suppose masses of emails get sent out to naive users saying the voting website has been changed and, after you submit your ballot and your credentials to the fake website, it helpfully votes for you, but changes some of the votes. You also have bots where millions of individual machines are controlled by a single person who uses them to send out spam. There is a program just sleeping on there waiting for somebody to come in and use it. Think about the consequences of that when it's time for an election. People would vote on their personal computers, not knowing that they were handing the ballot to a potential hostile middleman who could change the vote. And neither the voters nor election officials would see anything suspicious. Because of the secret ballot, there is no way for the voter to check that the ballot transmitted to the elections office is the one they filled out on their computer.

Just how disruptive could these risks become?

Without being paranoid, there are reasons to believe that people would want to affect the outcome of elections. Right now, they spend billions of dollars trying to do it through campaign contributions and advertising

and political consultants and all of that. It's like having a jewelry store. How good of an alarm system do you need for your jewelry store? Well, it depends how expensive your jewelry is. What is the value of controlling the U.S. presidency? There are people who would be very motivated to get something so valuable. Those people could include political zealots or campaigns, but they might also include organized crime or even other countries with huge resources.

How easy would it be to hack a computerized system? Not very hard, as we can see from the frequent news stories about massive thefts of data from government and corporate web servers. And there are many other threats, including voters who are not experts in computer security and may be easily fooled, and potential for corrupt insiders at companies that produce the internet voting software.

The way I look at things is: How many people have to conspire to steal an election now? With paper ballots at polling places, to steal a significant number of votes, you'd have to have lots of poll workers or a lot of voters voting fraudulently, which would be very difficult and expensive. And with paperless touchscreen voting you maybe need a few programmers. If you had widespread internet voting, on the other hand, the vulnerabilities are even more worrying.

Online voting could threaten the fundamental legitimacy of elections?

From the perspective of election trustworthiness, internet voting is a complete disaster. While you can't stop all election fraud, elections must have a higher standard of credibility. They need to have the perception of being low fraud. If you have an election system where fraud can be committed and – this is very important – that fraud is undetectable, then you don't really have a reason to trust the outcome of the election. And

that's very bad in a democracy, because the whole goal of an election is to satisfy the people who lost the election that they lost fair and square and that the candidate who is elected is legitimate.

Can you tell us about some of the challenges your organization, Verified Voting, is tackling?

The dangerous thing about internet voting is it appeals to a lot of people on the grounds that they use the internet for other stuff and it seems like voting should be easy. They don't stop to ask the computer scientists and don't even think it's controversial. Legislators say this sounds like a great idea and write a bill, and such bills have gotten passed without significant debate because it just seems like an obvious thing. There's no technical input. The challenge is: How do we raise people's awareness to the point where they can make an educated judgment about the risks of internet voting?

For instance, this year there were proposals for an internet voting initiative in California that made me shudder. I don't think it has gotten enough signatures to get on the ballot, so we're safe for a while. But ballot initiatives are something where it's very expensive to educate people enough on the problems of the technology. It's difficult enough to get legislators up to speed, much less the public. You're talking about millions of California voters who look at something on the ballot and say, "Oh, this sounds like a good idea." It could be a nightmare. I'm confident that if people actually do learn about it and take an objective look at the technology, they will conclude that it's not time yet.

Ultimately, is paper the gold standard we should stick to?

Yes. Paper has some fundamental properties as a technology that make it

the right thing to use for voting. You have more-or-less indelible marks on the thing. You have physical objects you can control. And everyone understands it. If you're in a polling place and somebody disappears with a ballot box into a locked room and emerges with a smirk, maybe you know that there is a problem. We've had a long time to work out the procedures with paper ballots and need to think twice before we try to throw a new technology at the problem. People take paper ballots for granted and don't understand how carefully thought through they are.

Provided by Stanford University