Testimony regarding touchscreen voting machines

Pennsylvania Senate Committee on Government, March 18, 2024

Andrew W. Appel

Good morning. I am a professor of computer science at Princeton University. I research and teach software verification, computer security, and technology policy; and for more than 20 years a significant part of my research is on the security of voting machines. Some counties in Pennsylvania, as well as some counties in my own state of New Jersey, are using touchscreen voting machines in a way that could severely compromise the trustworthiness of elections in the future. There's no evidence that anyone has used this security vulnerability to cheat in elections thus far, but I strongly recommend that Pennsylvania change to hand-marked paper ballots in all counties, and limit the use of touchscreen voting machines to those voters who cannot mark a paper ballot by hand.

Twenty years ago, many states and counties used paperless touchscreen voting machines, in which a computer program interpreted the voter's actions and then reported a vote total for each candidate when the polls closed. It is widely understood that this method has a severe security vulnerability: if a hacker manages to install a fraudulent computer program in the voting machine, that program can report fraudulent results. As a matter of computer science, it's not possible to totally prevent the installation of fraudulent software on a computer, including on a voting machine.

Between 2008 and the present, almost all states and counties have stopped using such machines, mainly because of the recognition of this security vulnerability. Therefore, over the past 10 years when citizens have questioned election results, the paper ballots have been there, available to recount; and in several states there *were* recounts or audits. If we want to be confident of election results without having to trust what software was loaded in a voting machine on a particular day, this is the way to do it.

But we can rely on a recount or audit of paper ballots only if the votes marked on the paper ballot are the choices that the voter actually indicated! When the voter marks a paper ballot with a pen, this goes without saying. But when the voter uses a touchscreen voting machine, a "ballot marking device", to create their paper ballot, then a hacked computer program can print votes onto the paper ballot that are not the candidates that the voter chose on the touchscreen. In fact, even if the voting machine is not hacked, if it's just misconfigured by accident, the ballot marking device sometimes prints the wrong names onto the paper ballot.

You might think, if the voting machine prints the wrong candidates onto the paper ballot, then the voter will notice that. But unfortunately, the average voter reviews their paper ballot printout for only about 2 seconds; and that if the voting machine deliberately prints a wrong vote onto the ballot then 93% of voters won't notice it.

You might think, at least if some voters notice that the voting machine is cheating, then a hacker can't get away with stealing an election. But no, actually. If you're a voter using a touchscreen ballot-marking-device to create your paper ballot, and the computer has printed votes onto the paper that were not your choices on the touchscreen, what are you supposed to do? You're supposed to tell the pollworker that the wrong votes are marked, and the pollworker is supposed to void that ballot and let you try again. But you can't prove to anyone that the computer mismarked your ballot. Whatever had been displayed on the touchscreen is long gone. You might be mistaken.

Now suppose a hacker has installed a fraudulent program that, in the contest for State Senator, alters 10% of the votes for candidate Smith to be votes for candidate Jones. And suppose 7% of the voters are careful enough to review every vote on the printed paper before depositing the ballot for counting, even down to the race for State Senate. That means one out of 140 voters will ask the pollworker for a do-over – four or five all day long in a typical polling place. But it also means that the voting machine has managed to shift the vote totals by 9.3%. So, a 58% landslide becomes a 49% loss. I hope you all won your elections by at least 58%.

Some voting machines encode the votes on the printed ballot using a barcode, and that's even worse. The voter has no way of knowing whether the barcode correctly records the candidates they chose on the touchscreen. And it's the barcode that will be counted by the optical scanner, not the human readable text. The whole point of a paper ballot is that it should be human readable, and barcodes defeat that.

There's a clear consensus among experts in the cybersecurity of voting that public elections should be conducted using hand-marked paper ballots, counted by optical-scan voting machines, and recountable or auditable by hand. Optical-scan voting machines are accurate and reliable, when they're not hacked. The purpose of random audits, or of recounts, is that if those optical scanners are ever hacked, or if they malfunction in some other way, the problem will be detected and corrected by recounting the paper ballots.

In contrast, with ballot-marking devices, hacks are difficult to detect and impossible to correct: the wrong votes have been marked onto the paper, and there's no way to correct that.

This really is the consensus among experts. I've provided to the committee a letter signed by 20 election cybersecurity experts, *Suggested Principles for State Statutes Regarding Ballot Marking and Vote Tabulation*.

Most Pennsylvania counties use hand-marked paper ballots, counted by machine and recountable by hand. That's the state-of-the-art most reliable method. But 14 counties are using touchscreen ballot-marking devices for all in-person voters, and that is a disaster waiting to happen. Now is the time to replace that equipment in those counties.