Philip B. Stark • Dept. of Statistics • University of California • Berkeley, CA 94720-3860

Rep. Alan Powell (Chair)
Rep. Barry Fleming (Vice Chair)
Rep. Rhonda Burnough
Rep. Joseph Gullett
Rep. Mary Frances Williams
Rep. Rick Williams
Rep. Bruce Williamson
Rep. Jay Powell (Ex-Officio)
Rep. Micah Gravley (Ex-Officio)
Subcommittee on Voting Technology of Government Affairs Committee
Georgia House of Representatives
Atlanta, GA

February 18, 2019

Ballot-marking devices (BMDs) are not secure election technology

Dear Chair Powell and members of the Subcommittee on Voting Technology:

I am Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley. I serve on the Board of Advisors of the U.S. Election Assistance Commission (EAC) and on the Board of Directors of Verified Voting Foundation. I invented "Risk-Limiting Audits," a method for checking whether reported election outcomes are correct, endorsed by the National Academy of Sciences, Engineering and Medicine; the Presidential Commission on Election Administration; the American Statistical Association; the League of Women Voters; Verified Voting Foundation; and other organizations concerned with election integrity. My CV is online at https://www.stat.berkeley.edu/~stark/bio.pdf

I write as an individual, not as a representative of my employer, the US EAC, or any other entity. The opinions expressed below are my own.

I advocate hand-marked paper ballots for voters who have the eyesight and dexterity to use them, and ballot-marking devices (BMDs) for those who need assistive technology—but not for all voters. I attach a letter expressing that opinion to Georgia's SAFE commission, signed by 24 experts in election integrity, security, and audits, including me.

There are many reasons I share this opinion, but the main issue is security: widespread use of BMDs makes voters responsible for ensuring that BMDs function correctly. However, BMDs do not provide voters a way to demonstrate to pollworkers or election officials that a BMD has malfunctioned, and the available evidence suggests that voters are not able to check BMDs effectively or reliably, as I shall explain. This makes auditing elections that were conducted primarily using BMDs meaningless: an audit could easily confirm an incorrect outcome, because a BMD-generated paper trail is not a trustworthy record of voter intent.

I believe these are the main considerations in hand-marked ballots versus BMDs:

1. **Mark legibility.** A properly functioning BMD will generate clean, unambiguous marks. However, experience with statewide recounts in Minnesota and elsewhere suggest that truly ambiguous handmade marks are very rare.[1] Thus mark legibility is not a good reason to adopt BMDs for all voters.
2. **Availability of accessible options.** If everyone voted on an accessible device, it would guarantee that an accessible device had been set up for voters who benefit from using one. This is not a good reason to adopt BMDs for all voters.
3. **Paper/storage.** BMDs that print summary cards rather than full-face ballots can save paper and storage space. That would be an advantage for BMDs, but for the security and cost issues. However, evidence suggests that the usability of summary cards to verify one's selections is very problematic, especially for long ballots with many contests. To my knowledge, there has been no testing of summary ballots or BMD-printed ballots for usability for voter verification.
4. **Cost.** Using BMDs for all voters substantially increases the cost of acquiring, configuring, and maintaining the voting system.
5. **Mechanical reliability and capacity.** Pens are likely to have less downtime than BMDs. It is easy and inexpensive to get more pens and privacy booths. If a precinct-count scanner goes down, people can still mark ballots with a pen; if the BMD goes down, voting stops.
6. **Security and responsibility.** I believe that a well designed and perfectly functioning BMD can help a voter avoid undervotes and other errors *as long as the device is trustworthy*. The problem is that no computer can be trusted to be running the software it is supposed to be running, nor can any software be trusted to be bug-free, especially in a high-stakes "critical infrastructure" role such as

[1] States do need clear and complete regulations for adjudicating voter intent from voter marks.

> recording and tabulating votes. BMDs have all the security and configuration vulnerabilities of the direct-recording electronic (DRE) devices currently used in Georgia. A voter might make his/her selections perfectly on the screen—and verify those selections—but the BMD could print something else on the paper, through error or malfeasance. Only the voter can check for that: auditors can only see what's on the paper. This is where security falls apart for BMDs. Universal use of BMDs makes every voter responsible for checking whether the BMD is functioning correctly, but a BMD does not give voters the evidence they would need to prove that a machine registered their vote incorrectly.[2] This is obviously a bad combination. According to the available evidence,
>
> - very few voters check the BMD printout
> - when they do, they generally do not notice errors
> - if they notice errors, shame or inconvenience might keep them from requesting another ballot
> - if they notice problems, there is no way for a voter to prove that the BMD printed the wrong thing, rather than that the voter erred, so there's no way to catch a cheating or misconfigured BMD
> - pollworkers are not trained to take a machine offline (and start a forensic investigation) if a number of voters complain that the BMD is printing their selections incorrectly.

Hence, the best-case scenario is that (some) voters who notice problems get to mark a new ballot. But if a bug, misconfiguration, or malicious hack caused a machine to swap, say, 30% of on-screen votes for Alice into printed votes for Bob, most of those swaps would not be noticed, and those that were noticed would be unlikely to trigger an investigation. There's no feedback mechanism to ensure that election officials find out that the machines are not performing as intended, to stop and repair the damage, or to prevent future damage.

Even worse, some BMDs (for instance, the ES&S ExpressVote XL with the "autocast" feature) can print on ballots after voters no longer have an opportunity to check what the ballot shows, making it completely impossible to catch errors or malfeasance in such a system.

Security design that relies on voters to check the equipment and programming is doomed. Good security design *allows* voters to check things, but does not *rely on them* to check that the equipment is functioning correctly. For this reason, widespread use of BMDs undermines election integrity, and I recommend hand-marked paper

[2] Auditors can check whether an opscan system is functioning correctly, but not whether the BMD printed the voter's selections correctly.

ballots for voters who have the dexterity and vision to use them.

Sincerely,

Philip B. Stark