

Latest Threat to Democracy: Barcodes, Ballot Marking Devices (a.k.a. 'Electronic Pencils')

As unverifiable touchscreen DREs are phased out of our nation's voting systems, unverifiable touchscreen BMDs ('Son of DREs') are on the way...

By [JENNIFER COHN](#) on 3/12/2018, 9:45am PT

[An earlier version of this article was [originally published](#) by Jennifer Cohn at Medium.]

A Ballot Marking Device ("BMD") is a **touchscreen** computer that generates a **computer-marked** paper ballot or printout, which is then tallied on a computerized optical scanner. (Those computer-marked ballots can also, in theory, be counted by hand, but generally are not, as most election officials rely on optical scanners instead.)

BMDs were initially designed for people who are **unable** to **hand-mark** paper ballots due to disability, old age, etc. But the state of [Georgia](#) and [Los Angeles County, California](#) are now at the forefront of an unfortunate new trend, which is to consider buying these expensive hackable "electronic pencils" for use by **all** voters at the polls, regardless of need.

The Georgia legislature is quickly working to adopt a bill to fund such new systems to replace their similarly 100% unverifiable, 15-year old Diebold touchscreen systems used across the entire state. L.A. County is in the late process of a years-long development program to deploy these systems in time for the 2020 Presidential election.

Should Georgia and Los Angeles proceed on their current course, it would introduce a **second** unnecessary and insecure computer system in the polling place above and beyond already insecure optical scanners, creating **twice** as many opportunities for electronic programming errors, paper jams, and hacking. For example, some BMD systems have already had problems with:

- Vote flipping (when election integrity advocate and journalist Brad Friedman used such a device in Los Angeles in a 2008 election, the device [flipped 4 out of 12 of his selections](#) on the computer-marked paper ballot);
- Inability to display all candidates on one screen (a problem [reported by the state of Maryland](#), which had acquired such systems for all voters, but changed its mind even though the screen problem was eventually fixed); and
- Vendor breach of certification requirements (as [occurred with vendor Election Systems & Software](#), "ES&S", the nation's largest voting system vendor).

Meanwhile, two of the most popular BMD's --- the ES&S ExpressVote and the Dominion ImageCast --- produce **bar-coded** (or QR-coded) printouts, which cannot be read by human beings, in lieu of traditional, hand-marked paper ballots.

This is alarming, according to experts --- including some who describe BMDs as "Son of DREs" --- for a number reasons...





Voting system experts and computer scientists **warn** "barcodes on ballots...could give hackers a chance to rewrite results in ways that could not be traceable..." As longtime Finnish computer security expert Harri Hursti **explained** to President Trump's Commission on Election Integrity late last year, "certain vendors include barcodes into the ballots, and proper studies [to] my knowledge have not been made," despite "the recent understanding [of] how to use barcode as an attack vector." Also, the human-readable portion of the BMD printout --- which is supposed to correspond with the voter's selections on the touchscreen --- is not what the optical scan computers actually count when they tally results. Rather, the scanners read *only* the bar-coded portion of the printouts, which humans cannot read!

Moreover, the uncounted human-readable portion of the printout cannot even be considered "**verified**" unless voters actually know and take the time to review it. But even *that* is not quite as simple as proponents of BMDs might have you believe.

A Las Vegas survey **found**, for example, that "**fewer than 40 percent of voters actually checked the paper record of their vote before leaving the polling place.**" Although the study concerned so-called "Voter-Verifiable Paper Audit Trails" ("VVPATs") from Direct Record Electronic ("DRE", usually touchscreen) voting machines, there is no basis to assume that voters would be more inclined to check the paper records produced by BMDs.

Meanwhile, a **Rice University study [PDF]** of computer "review screens", summarizing the voter's selections at the end of the voting process, found that "**over 60% of voters do not notice if their votes as shown on the review screen are different than how they were selected.** Entire races can be added or removed from ballots and voter's candidate selections can be flipped and the majority of users do not notice."

While that study examined review screens, its alarming findings bode poorly for BMD printouts. Similar to the computer screens, BMD printouts are printed *only after* voters have made *all* of their selections. The printout happens at the very end of the long voting process, thus requiring voters to tax their memories --- without the benefit of being able to go back and review their selections on screen. Although voters may easily remember the top of the ticket races, they are unlikely to readily recall the many races and referenda further down the ballot, much less notice any discrepancies between the BMD printouts and their intended selections.

And here's the kicker. Even if voters discover such discrepancies, they are unlikely to do anything about it. Professor Ted Selker of MIT **reports** that, "In watching 500 voters casting ballots, **I saw less than one in 10 people who, when they were told they had a problem with their ballot, were actually willing to take a new ballot and vote again.**"

[Friedman adds even one more kicker: "After the election, in the case of any challenge, there is no way to know that *any* computer-marked ballot has been reviewed by *any* voter, correctly or otherwise," he says. "Thus, there is no way to know that *any* ballot reviewed by humans in the event of a recount or so-called audit actually reflects the will of *any* voter. We're back to the same 100% unverifiable type of voting system that Georgia is currently planning to replace."]

Thus, even if computer-marked paper ballots are a necessary accommodation for those who are unable to hand-mark their ballots, it would be utterly irresponsible to make them the primary system for all voters. In the wake of the Help America Vote Act of 2002 ("HAVA", which allocated billions of dollars for new voting systems following the 2000 Presidential debacle), some [advocates](#) and [elected officials](#) cited the disabled community as a [pretext](#) for the purchase of insecure paperless Direct Recording Electronic ("DRE") voting machines [for all voters](#).

States --- such as Georgia, Maryland and [many others](#) --- thus rushed to buy these insecure, unverifiable machines in large numbers, padding the pockets of private vendors and lobbyists, while creating a 15-year disaster of election integrity. Others in the disabilities community have since [called for](#) the elimination of all DREs.

We must learn from our nightmarish, and still-ongoing experience with DREs and not make the very same mistake with BMDs in replacing them and other hand-marked paper based systems. As one election integrity advocate in Georgia recently [quipped](#): "They joke with the press about \$5,000 pencils (which is horrifying enough) but nobody points out the obvious: real pencils can't be hacked."

* * *

UPDATE: Soon after I posted a link on Twitter to the original version of this article [at Medium](#), a high ranking Colorado official dismissed as "anecdotal" the BMD vote-flipping experience by Friedman as referenced at the start of the article, advising that he has neither seen nor heard of such problems in Colorado. He did not dispute Hursti's concern about barcodes, but implied that his state's post-election risk limiting "audits" ("RLAs") rendered moot any concerns about either hacking or programming error.

I disagree. Although Colorado recently test-piloted RLA's statewide, most states [do not require](#) --- nor frequently even allow --- meaningful post-election audits. And, even if they did, it would be irresponsible to allow the widespread use of unnecessary, expensive, and insecure BMD's predicated on the notion that meaningful post-election audits --- *if* properly conducted --- "should" be able to detect tampering. No thank you. Jurisdictions should try to preclude systems [that allow for](#) invisible manipulation and even programming errors from happening in the first place, as well as conduct robust manual post-election audits. This should not be an either/or proposition.

* * *

Jennifer Cohn is an attorney and election integrity advocate in the San Francisco Bay Area who graduated from UCLA and Hastings College of the Law. As an attorney, her areas of practice included insurance coverage and appellate law. She practiced law for more than twenty years, including seven years as a partner with Nielsen Haley & Abbott, LLP in Marin County, California. Since 2016, she has devoted her professional efforts full time toward investigating our insecure election system and potential solutions. She can be contacted through her Twitter account, [@jennycohn1](#).

<http://bradblog.com/?p=12505>