

**IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

DONNA CURLING, et al.

Plaintiff,

vs.

BRIAN P. KEMP, et al.

Defendant.

**CIVIL ACTION FILE NO.: 1:17-cv-
2989-AT**

THIRD SUPPLEMENTAL DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my declarations of September 9, 2018, September 30, 2018, and October 22, 2019. I stand by everything in the previous declarations.
2. I have read portions of the State Defendants' Combined Response in Opposition to Curling Plaintiffs' and Coalition Plaintiffs' Motions for Preliminary Injunction, dated November 13, 2019 ("Combined Response"). This declaration responds primarily to assertions made in the Combined Response, including the declaration of Juan E. Gilbert, Ph.D., contained therein ("the Gilbert declaration").

AUDITS

3. The most compelling reason for post-election audits is to provide public evidence that the reported outcomes are correct, so that the electorate and the losers' supporters have reason to trust the results. Audits that cannot provide evidence that outcomes are correct

are little comfort. A transparent, full hand count of a demonstrably trustworthy paper record of votes can provide such evidence. So can a risk-limiting audit of a demonstrably trustworthy paper record of votes. The advantage of risk-limiting audits is that they are often more economical and efficient than a full hand count; the disadvantage is that they can fail to correct a wrong outcome. What makes an audit “risk limiting” is that the chance it fails to correct a wrong outcome is guaranteed not to exceed a pre-specified limit, the “risk limit.”

4. Indeed, by definition, a risk-limiting audit must have a known minimum chance of correcting the reported outcome if the reported outcome is incorrect. A risk-limiting audit corrects the reported outcome by conducting a full manual tabulation of the votes in the paper trail: just like a recount, it requires a trustworthy paper trail. If there is no trustworthy paper trail, a true risk-limiting audit is not possible, because an accurate full manual recount would not necessarily reveal who won. Because BMD printout is not trustworthy, applying risk-limiting audit procedures to BMD printout does not yield a true risk-limiting audit.
5. Defendants assert that a post-election audit can demonstrate that BMDs function correctly during elections. As I wrote in my October 22, 2019, supplemental declaration, audits of BMD-marked ballots (printouts) cannot reliably detect whether malfunctioning BMDs printed the wrong votes or omitted votes or printed extra votes. (Here, as before, I use the term *malfunction* generically to include problems due to bugs, configuration errors, and hacking.) As I wrote then, that is true even if the malfunctions were severe enough to make losing candidates appear to win.

6. Applying risk-limiting audit (RLA) procedures to securely curated BMD printouts can check the accuracy of the tabulation of the printouts. It can provide confidence that if errors in scanning and tabulation were large enough to change the reported winner(s), that fact would be detected and corrected.
7. But such an audit does *nothing* to check whether the BMDs printed incorrect votes, omitted votes, or printed extra votes. Risk-limiting audit procedures check the *tabulation of BMD printouts*; they do not check the *functioning of the BMDs*. They cannot confirm the outcome of elections conducted using BMDs.
8. Indeed, there is no known pre-election or post-election procedure that can tell reliably whether BMDs will malfunction or did malfunction during an election. Nor is there any practical procedure that can reliably detect outcome-altering BMD malfunctions during an election.¹
9. Therefore, there is no way to establish that BMD printout is a trustworthy record of what the BMD displayed to the voter or what the voter expressed to the BMD.
10. While it is crucial to maintain secure custody of the election paper trail—whether the paper trail consists of hand-marked ballots or BMD printouts—even if BMD printouts have been maintained verifiably securely, they are not a trustworthy record of what voters did, what they saw on the BMD screen, or what they heard through the BMD audio interface, because there is vulnerable software between the voter and the printout. In contrast, computer hacking, configuration errors, and bugs cannot cause pens to put the wrong marks on hand-marked paper ballots.

¹ Stark, P.B., 2019. There is no reliable way to detect hacked ballot-marking devices. ArXiv, <https://arxiv.org/pdf/1908.08144.pdf> (last visited 20 October 2019).

11. Voters can err in hand-marking ballots and in using a BMD. But BMD printouts are also vulnerable to bugs, misconfiguration, and hacking; hand-marked paper ballots are not.
12. The tabulation of both kinds of paper record is subject to bugs, misconfiguration, and hacking. Rigorous audits can ensure (statistically) that tabulation errors did not alter the reported outcomes. But they cannot ensure that errors in BMD printouts did not alter the reported outcomes.
13. Some voters check their BMD printouts, and, if they notice errors, will request a fresh opportunity to vote. But unless virtually every voter diligently checks the printout before casting it, there is no reason to believe that an accurate tabulation of BMD printouts will show who really won.
14. The evidence suggests that less than ten percent of voters check their printouts, and that voters who do check often overlook errors. See paragraph 30(d), *infra*. As a result, errors in universal-use BMD printouts could alter margins by very large amounts: virtually every contest is decided by fewer votes than undetected, uncorrected errors in BMD printouts could produce.
15. But even if ninety percent of voters check their printouts and correct any errors they find, misprinted votes on the remaining ten percent of printouts could alter a reported margin by twenty percent (or even more than twenty percent, for contests that are not on every ballot). Many contests are decided by margins of less than twenty percent.
16. In an actual election, there is no way to know how many voters checked their BMD printouts for accuracy.

THE NOVEMBER 2019 PILOT RISK-LIMITING AUDIT IN GEORGIA

17. I invented risk-limiting audits in 2007 and published the first peer-reviewed papers about them in 2008.² I collaborated with election officials in California and Colorado to conduct the first dozen or so pilot RLAs, starting in 2008.³ In 2011, I invented and published the particular RLA method⁴ used in the 2019 pilot audit of two contests in Cartersville, Georgia, conducted with the assistance of Verified Voting and VotingWorks.⁵ (I was not involved in the Cartersville pilot audit.) The method, “ballot polling,” was published more formally in 2012 in two peer-reviewed papers I co-authored.⁶ I provided open-source software implementing ballot-polling RLAs,⁷ which became the basis of the State of Colorado RLA regulations, the software the State of Colorado currently uses for its audits, and the Arlo software used for the Georgia pilot audit. Indeed, I understand that VotingWorks, the company that built the Arlo audit

² Stark, P.B., 2008. Conservative statistical post-election audits, *The Annals of Applied Statistics*, 2, 550–581. Reprint: <http://arxiv.org/abs/0807.4005>

Stark, P.B., 2008. A Sharper Discrepancy Measure for Post-Election Audits, *The Annals of Applied Statistics*, 2, 2008, 982–985. Reprint: <http://arxiv.org/abs/0811.1697>

³ Hall, J.L., L.W. Miratrix, P.B. Stark, M. Briones, E. Ginnold, F. Oakley, M. Peaden, G. Pellerin, T. Stanionis and T. Webber, 2009. Implementing Risk-Limiting Audits in California, *2009 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '09)*

⁴ <https://www.verifiedvoting.org/philip-stark-report-on-second-risk-limiting-audit-under-ab-2023-in-monterey-county-california/> (last visited 9 December 2019).

⁵ Mark Lindeman, Verified Voting, personal communication, 9 December 2019.

⁶ Lindeman, M., P.B. Stark, and V.S. Yates, 2012. BRAVO: Ballot-polling Risk-Limiting Audits to Verify Outcomes. *2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '12)*

Lindeman, M., and P.B. Stark, 2012. A Gentle Introduction to Risk-Limiting Audits. *IEEE Security and Privacy*, 10, 42–49.

⁷ <https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm> (last visited 12 December 2019).

software, used my software as a touchstone to ensure that they had implemented the method correctly.⁸

18. Ballot-polling audits are a bit like exit polls, but instead of asking randomly selected voters how they voted, they manually inspect randomly selected cast ballots to see the votes they contain. If a large enough random sample of ballots shows a large enough majority for the reported winner(s), that is strong statistical evidence that the reported winner(s) really won. It would be very unlikely to get a large majority for the reported winner(s) in a large random sample of ballots if the true outcome were a tie, or if some other candidate(s) had won. There is deep mathematics behind proving out how large is “large enough” to control the risk to a pre-specified level, such as five percent. However, the calculations that determine when the audit can stop examining more ballots are relatively simple.
19. No auditing method can check whether BMD printout correctly recorded voters’ expressed intent.
20. Ballot polling, the audit method used in Cartersville, does not check whether any BMD printout was tabulated correctly. Ballot-polling audits only check whether a full hand count of the BMD printout would find the same winners. In particular, the vote tabulation system in Cartersville could have mistabulated every single BMD printout and still passed the audit.
21. The Cartersville pilot audit did not—and in principle could not—confirm that the reported outcomes were correct, because it did not and could not show that the BMDs functioned correctly. All the audit did was provide statistical evidence that a full manual

⁸ Ben Adida, VotingWorks, personal communication, 8 November 2019.

tabulation of the BMD printouts would find the same winners that were reported in the two audited contests. If the BMD printouts contained outcome-changing errors, the audit would have had no chance of detecting that, nor of correcting the reported outcomes.

22. In contrast, if the election had been conducted with hand-marked paper ballots and those ballots had been properly secured, the same audit procedure could have provided strong evidence that the reported winners really won.

23. I resigned from the Board of Directors of Verified Voting Foundation over their president's refusal to clarify publicly that the Cartersville pilot audit did not "confirm outcomes" or show that the voting system worked correctly.

THE NATIONAL ACADEMIES REPORT

24. Defendants claim that the 2018 National Academies of Science, Engineering, and Medicine report *Securing the Vote: Protecting American Democracy* ("NASEM Report") recommends BMDs. In fact, the NASEM Report draws important distinctions between BMDs and hand-marked paper ballots, and points out that additional research on BMDs should be conducted before BMDs are deployed widely:

- a. "The U.S. Election Assistance Commission, National Institute of Standards and Technology, U.S. Department of Homeland Security, National Science Foundation, and U.S. Department of Defense should sponsor research to: [] determine voter practices regarding the verification of ballot marking device-generated ballots and the likelihood that voters, both with and without disabilities, will recognize errors or omissions[.]" NASEM Report, at 11–12.

- b. “Research suggests that DRE VVPATs⁹ tend not to be voter verified. This suggests that VVPATs may be of little value as a check on the accuracy of DREs. See, e.g., Everett, S. P., “The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection,” doctoral dissertation, Rice University, Houston, Texas and Campbell, Bryan A. and Michael D. Byrne, “Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability,” Proceedings of EVT/WOTE, 2009. Research on the rate of voter verification of BMD ballots relative to the rate of verification of VVPATs or voter-marked paper ballots has been limited.” NASEM Report, at 44.
- c. “Unless a voter takes notes while voting, BMDs that print only selections with abbreviated names/descriptions of the contests are virtually unusable for verifying voter intent.”¹⁰ NASEM report, at 79.
- d. “By hand marking a paper ballot, a voter is, in essence, attending to the marks made on his or her ballot. A BMD-produced ballot need not be reviewed at all by the voter. Furthermore, it may be difficult to review a long or complex BMD-produced ballot. This has prompted calls for hand-marked (as opposed to BMD-produced) paper ballots whenever possible.” NASEM Report, at 79.

25. Recent congressional testimony of Dr. Matt Blaze of Georgetown University¹¹ echoes these concerns:

⁹ VVPAT stands for “voter-verified paper audit trail,” a printout similar to a cash register receipt that some DREs provide. As explained by NASEM, such receipts are rarely “verified” by voters: the acronym is a misnomer.

¹⁰ I understand that the BMDs Georgia is using are of this type.

¹¹ Blaze, Matt. Testimony Before the US House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation. Hearing on Defending Against Election Interference, November 19, 2019.

“BMD-based voting systems are controversial, since, by virtue of their design, the correctness of their behavior cannot be effectively audited except by every individual voter carefully verifying his or her printed ballot before it is cast. A maliciously compromised BMD could subtly mismark candidate selections on ballots in a way that might not be noticed by most voters. If BMDs fail or must be rebooted at a polling place, there may be no way for voters to create marked ballots, making BMDs a potential bottleneck or single point of failure on election day.

As a relatively new technology, BMD-based systems have not yet been widely examined by independent researchers and have been largely absent from practical election security research studies. However, even with relatively little scrutiny, exploitable weaknesses and usability flaws have been found in these systems. This underscores the need for more comprehensive studies and for caution before these systems are purchased by local jurisdictions or widely deployed.” Blaze testimony, at 8.

26. Defendants claim that “Plaintiffs cannot point to any real security risk or hacking potential the use of BMDs poses.” There are countless studies showing that BMDs and other electronic voting equipment have serious security vulnerabilities and can be hacked. The 2018 Def Con Voting Village Report found easily exploited vulnerabilities in the

<https://www.congress.gov/116/meeting/house/110238/witnesses/HHRG-116-HM08-Wstate-BlazeM-20191119.pdf> (last visited 12 December 2019).

Dominion ImageCast Precinct BMD,¹² which I understand is of the same make that Georgia has deployed, but possibly not the identical model.

DR. GILBERT'S DECLARATION

27. Dr. Gilbert questions my credentials regarding election security, dismissing me as a statistician. I am on the cybersecurity subcommittee of the Board of Advisors of the U.S. Election Assistance Commission. I have authored or co-authored more than 15 peer-reviewed articles in journals and conference proceedings on cybersecurity, information forensics, and the security of electronic voting technology; my co-authors are an international who's-who of cybersecurity experts and cryptographers. I have been a keynote speaker at numerous international conferences on cybersecurity and elections. I have given two distinguished lectures at the Center for Security, Reliability, and Trust at the University of Luxembourg. I am the co-author of a report on election forensics for the Venice Commission of the Council of Europe. I have testified to the California legislature on election security several times, and to the California Little Hoover Commission. I have advised the California Secretary of State and the Colorado Secretary of State on mitigating electronic threats to elections. I have advised the governments of Denmark, Nigeria, and Mongolia on election security. I have been a Visiting Professor of Theoretical Computer Science at the IT University of Copenhagen, sponsored by a Velux/Villum Foundation fellowship to work on election cybersecurity. I am regularly on the program committee of two international election security conferences. And, as

¹² <https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf> at 18–19. (last visited 12 December 2019).

mentioned above, I invented risk-limiting audits, widely regarded to be the best tool for verifying election outcomes even in the face of hacking and computer malfunctions (provided there is a trustworthy paper trail of votes).

28. Dr. Gilbert’s expertise related to elections is in usability. He does not represent himself to be an expert in computer security, statistics, or auditing. I have read his CV dated 24 November 2019.¹³ His research focuses on usability, accessibility, inclusion, and the use of technology in teaching and mentoring, for instance, making self-driving cars more accessible, inclusive university admission policies, using “chatbots” to mentor graduate students, “designing a humorous workplace,” cyberbullying, and similar subjects. He has two refereed paper related to electronic voting in 2012 and 2013. Both are usability studies, not security studies. His only publication in a security-related journal was in 2008, with eight co-authors, introducing a BMD system he helped design. That paper describes the system and some measures they took to secure it but does not include a formal security analysis of the system. He published a paper on risk analysis of software design (not implementation) with three co-authors, in what appears to be an Alabama-based industrial trade show in 2012.¹⁴ I was unable to find a copy of that paper. His credentials in cybersecurity are limited and inapposite.

29. Many of Dr. Gilbert’s pronouncements on security and auditability of BMD systems are erroneous. I shall not rebut them all, but I shall point out a few particularly serious errors.

¹³ <https://www.cise.ufl.edu/~juan/cv.pdf> (last visited 14 December 2019)

¹⁴ AlaSim: <https://10times.com/alasim> (last visited 14 December 2019) “The annual AlaSim International Conference & Exposition showcases the vibrant, multi-domain, modeling and simulation (M&S) industry in Alabama.”

30. Defendants claim, partly on the basis of Dr. Gilbert’s declaration, that “BMDs are far more like hand-marked paper ballots than they are like DREs.” Combined response, at 2; Gilbert declaration, at 11ff. That is not true from the perspective of technology, security, auditability, or evidence. The only thing BMDs have in common with hand-marked paper ballots is that both involve paper tabulated by scanners, while DREs tabulate directly from an electronic record. Aside from that, BMDs (and their attendant risks) are exactly like DREs with VVPAT:

- a. Vulnerable electronic technology is between the voter and the vote record: the paper trail itself is hackable. There is no trustworthy record of the voter's expressed vote with either technology. Both BMDs and DREs can be hacked—from afar, undetectably. Pens have no software to hack.
- b. In contrast to Defendants’ claim that for BMDs (and, by implication, DREs) “there are no questions of voter intent” (Combined Response, at 2), BMDs *obscure all direct evidence* voter intent. This is an example of “the ostrich principle”: because BMDs make the problems impossible to detect, Dr. Gilbert concludes that the problems do not exist. It is impossible to know from BMD printout what the voter expressed to the machine or what the BMD presented to the voter on the screen or audio interface. In contrast, voter intent can generally be inferred manually from voters’ marks on hand-marked paper ballots.¹⁵
- c. There is no way a voter can prove that a BMD or DRE printed his or her vote incorrectly, so the underlying “security loop” for both technologies is broken in

¹⁵ See the discussion of the Minnesota recounts in Appel, A., R. DeMillo, and P.B. Stark, 2019. Ballot-marking devices (BMDs) cannot assure the will of the people, SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375755 (last visited 20 October 2019).

the same way. Neither system generates any evidence a voter can take to an authority or third party to demonstrate that there was a problem.

- d. All extant research of which I am aware suggests that voters rarely check BMD printout or DRE printout, and that voters are not good at catching errors in the printout when they do check.¹⁶
- e. Neither DREs nor BMDs are auditable in practice. Pre-election logic and accuracy testing cannot assure that the devices will perform properly on election day. No practical amount of parallel or “live” testing on election day can provide reasonable assurance that the devices record votes accurately.¹⁷ No post-election procedure can determine whether the devices correctly recorded votes during the election.
- f. A DRE can be converted into a BMD by adding a printer and making changes to the software. And a BMD can be converted into a DRE by means of changes to the software alone. The same is not true for hand-marked paper ballots.

31. Dr. Gilbert opines that various properties of BMDs make them preferable, on balance, to hand-marked paper ballots. Gilbert declaration, at 11. His declaration generally does not address the security aspects of BMDs, which are at the heart of the issue. Many of his opinions are contradicted by the available data and by his own research.

32. Most of the advantages he claims universal-use BMDs have over hand-marked paper ballots fall into four categories:

¹⁶ In addition to the studies cited by Appel et al. (2019), I am aware of another study of whether and how well voters check BMD printout that is currently in peer review.

¹⁷ Stark, P.B., 2019.

- a. *They are not actually advantages.* Issues of ballot layout and design are in this category: bad layout can greatly increase voter errors for both BMDs and hand-marked paper ballots. Indeed, his own work points out examples where bad screen layout and bad user interfaces in touchscreen voting equipment evidently caused a high undervote rate.¹⁸ Undervote protection also falls partly in this category: both BMDs and precinct-count optical scan hand-marked paper ballots can offer protection against undervotes and overvotes (depending on system configuration); however, BMDs offer an “attack surface” that would allow malware to insert votes in contests the voter deliberately chose not to vote in. That cannot occur with hand-marked paper ballots.
- b. *They ride on a misuse of terminology.* For instance, he conflates “ambiguous mark” with “a mark a scanner cannot read.” Similarly, his conclusion that hand-marked paper ballots are not strongly software independent ignores part of the definition of strong software independence. And he conflates auditing the tabulation of votes with auditing electoral outcomes—which requires a trustworthy paper record of the votes.
- c. *The claimed advantages occur only if the BMDs function correctly.* Usability and overvote and undervote protection also fall partly in this category. The primary problem with BMDs is that there is no way to ensure that they function correctly. They are vulnerable to bugs, misconfiguration, and malicious hacking. This was brought home in the recent election in Northampton, PA, where BMDs were

¹⁸ Gilbert, J.E., J. Dunbar, A. Ottley and J.M. Smotherman, 2013. Anomaly detection in electronic voting systems, *Information Design Journal*, 20(3), 194–206, at 195–196.

miscalibrated and misconfigured. The configuration errors—which were not discovered by pre-election logic and accuracy tests—were so severe that *voter instructions* (rather than candidates) *received thousands of votes!*¹⁹

- d. *The advantages might occur for some BMD systems but not others.* Usability advantages fall in this category: he makes blanket statements that BMDs are usable by voters with disabilities. Gilbert declaration, at 19. A number of BMDs have failed usability testing in other states.²⁰ (Moreover, increases in usability in recording selections electronically are largely undermined, because the equipment cannot be relied upon to print those selections accurately.) Gilbert makes blanket statements about the usability of By his own admission, he has not inspected the BMD system Georgia is deploying. Gilbert declaration, at 16, 20.

33. I now give more specific examples of incorrect security assessments he made.

34. Dr. Gilbert overlooks the fact that BMD printouts have every security vulnerability that hand-marked paper ballots do, *plus* cyber risks that cannot feasibly be mitigated. In

¹⁹ “An instructional message regarding cross-filed candidates created an error in the machines’ database. As a result, thousands of electronic votes were mistakenly cast for the instructional message instead of the correct candidate.” [T. Shortell](#) and [Christina Tatu](#), *The Morning Call*, 12 December 2019. <https://www.mcall.com/news/elections/mc-nws-northampton-county-election-voting-machine-problems-reason-20191212-6icnnb2fqjfw5dencuy73n66wm-story.html>, last visited 13 December 2019. According to this report, the manufacturer admits that 30% of the machines were misconfigured—and that the misconfiguration was not detected by pre-election logic and accuracy testing.

²⁰ For instance, the Dominion Democracy 5.5 system, including the ImageCast Precinct and the ICX Prime BMD, failed testing in Texas for reasons of security and accessibility. https://www.sos.state.tx.us/elections/laws/jan2019_dominion.shtml (last visited 14 December 2019). The ES&S ExpressVote and ExpressVote XL BMDs failed usability testing in Pennsylvania with several “show stopper” flaws; moreover, the review found that it was “possible but challenging” to verify the BMD printout: <https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/ESS%20EVS%206021/EVS%206021%20Secretary%27s%20Report%20Signed%20-%20Including%20Attachments.pdf> (last visited 14 December 2019)

particular, he makes much of risks involving the physical security of hand-marked paper ballots but ignores the fact that BMD printouts face the same physical security risks (and additional cyber risks).

35. Dr. Gilbert ignores the fragility and unreliability of BMDs and the fact that BMDs produce a bottleneck in the voting process.²¹ There are many instances where voting machines did not boot up or misbehaved on election day, preventing voting or undermining voter confidence.²² Providing an inadequate number of BMDs in polling places will also discourage or prevent voting by creating long lines.
36. He treats risks that require a large conspiracy, insider malfeasance, and physical access to ballots as if they were equivalent to cyber risks, where nation states—or individual hackers—can undetectably alter election results without physical access to any part of the voting system. The primary threats to hand-marked paper ballots are of the first kind. BMDs face exactly the same threats of the first kind, but also face threats of the second

²¹ See paragraph 25, *supra*.

²² There are many examples of election equipment failures and malfunctions on election day. Here are a few, including some failures of relatively new or brand new equipment:
<https://www.mcclatchydc.com/news/politics-government/election/midterms/article221196655.html> (last visited 16 December 2019)
https://www.postandcourier.com/free-times/news/local_and_state_news/richland-county-failed-to-count-hundreds-of-november-election-ballots/article_849a1c98-c21a-5728-afc5-c58aae39e126.html (last visited 16 December 2019)
<https://www.commoncause.org/media/south-carolina-voting-machine-failure-undercores-need-for-swift-federal-action-for-voting-security/> (last visited 15 December 2019)
<https://www.pennlive.com/news/2019/11/gop-officials-file-legal-action-in-pa-after-massive-voting-machine-malfunctions-ballots-placed-in-suitcase.html> (last visited 15 December 2019)
<https://www.kansascity.com/news/politics-government/election/article221198575.html> (last visited 16 December 2019) <https://www.pbs.org/newshour/politics/which-states-were-hit-by-voting-problems-on-election-day> (last visited 16 December 2019)
<https://www.montgomeryadvertiser.com/story/news/2017/12/12/new-voting-machines-cause-senate-election-problem-montgomery-polling-place/944247001/> (last visited 16 December 2019)
https://www.upi.com/Top_News/US/2018/10/26/Texas-voters-report-error-with-electronic-voting-machines/9211540569616/?ilink=1 (last visited 16 December 2019)

kind that cannot be controlled by auditing. His discussion of “undervote hacks” and “overvote hacks” on hand-marked paper ballots commits this error.

37. He implies—contrary to the evidence and contradicting his own publications—that voters will catch and correct errors in BMD printout. Every extant study I know of finds that voters rarely check BMD printout, and that when they check, they often fail to notice errors that are present. This is consistent with research on DRE printouts also.²³ His own publications cite research that “no more than half of study participants notice [voting machine] review screen anomalies.”^{24,25}

38. He claims that BMDs and hand-marked paper ballots are equally auditable. The *tabulation* of both kinds of paper record can be audited, but no practical amount of auditing can offer any assurance that *BMDs themselves* did not malfunction and were not hacked to produce erroneous paper records.²⁶

39. The advantages Dr. Gilbert claims BMDs have (undervote and overvote protection, accessibility, etc.) are predicated on the BMDs functioning correctly. But that is precisely the problem: BMDs cannot be relied upon to function correctly, nor is there a reliable way to detect malfunctioning BMDs. Moreover, if BMD malfunctions are detected, there is no way to determine which printouts were affected and what the correct electoral outcome is. The only remedy is to hold a new election.

40. Dr. Gilbert’s analysis of overvote and undervote protection assumes that what BMDs print is identical to what the BMD shows voters on the screen or presents voters through

²³ See paragraph 24(b), *supra*, and note 16, *supra*.

²⁴ Gilbert et al., 2013.

²⁵ Of course, noticing an anomaly on a review screen and noticing an anomaly on BMD printout are not the same task, and a BMD can print something other what the review screen shows.

²⁶ Stark, P.B., 2019.

audio. That ignores the possibility of BMD malfunctions and hacking. A BMD can print selections that differ from what the voter was presented on the screen or the audio interface. It can omit contests or votes, add contests and votes, and alter votes. BMDs provide *no* protection against overvotes and undervotes created by BMD malfunctions. Dr. Gilbert assumes away the essential problem: BMD technology is not trustworthy.

41. Dr. Gilbert alleges that there is no effective protection against overvotes or undervotes in hand-marked paper ballot systems. In fact, many, if not all, precinct-count optical scan systems for tabulating hand-marked paper ballots can warn voters of undervotes and overvotes, and can return the ballot to the voter if the voter wishes to re-mark the ballot in response, or allow the voter to override the warning and cast the ballot.
42. BMDs are vulnerable to “presentation attacks,” where bugs, misconfiguration, or hacking causes the device not to display a contest the voter has a right to vote in (denying the voter the opportunity to vote in that contest). This can *create* undervotes that the BMD would not help the voter “detect.” While contests might be omitted from pre-printed paper ballots, standard pre-election procedures can detect that. In contrast, there is no practical procedure—before, during, or after the election—that can provide a reasonable level of assurance that a BMD presented voters the correct opportunities to vote.
43. Dr. Gilbert’s concern about “undervote hacks” identifies an important problem with all paper-based systems, including BMDs: the paper trail must be kept demonstrably secure from additions, subtractions, substitutions, and alterations. That is just as true for BMD printouts as it is for hand-marked paper ballots. A crucial difference he omits, however, is that altering hand-marked paper ballots is intrinsically a “retail” fraud problem: it takes many people, a lot of time, and physical access to the ballots to alter a large number of

ballots. In contrast, BMD printouts are subject to “wholesale” fraud and error as a result of bugs, hacking, or misconfiguration. It does not require many accomplices or physical access to the voting system or the printouts to alter outcomes of elections conducted on BMDs.

44. He expresses concern that systems that lack undervote protection (meaning hand-marked paper ballots) will have disparate impact on minority voters, citing experience in 2000. Gilbert declaration, at 27. More recent data belie this claim. I understand that the DREs in use in Georgia in the 2018 election had undervote protection. But the rate of undervotes in the 2018 Lt. Governor’s contest was much higher for voters who used DREs than it was for voters who used hand-marked paper ballots, including ballots cast by mail, which do not have undervote protection. That differential undervote rate was generally *higher* in precincts with higher percentages of Black voters, by an amount that was large and statistically significant.²⁷
45. Dr. Gilbert says that BMDs avoid the problem of ambiguous marks. Gilbert declaration, at 18, 29. That is true, but misleading. First, while BMD marks might be unambiguous, they are not trustworthy. *Voter intent on BMD printouts is entirely ambiguous*. No BMD mark can be trusted to represent what the voter expressed to the BMD or what was presented to the voter on the review screen or audio interface. Second, he confuses “ambiguous” with “not machine readable.” Some handmade marks are not machine readable, but marks that are ambiguous to human readers are evidently rare. For instance,

²⁷ Ottoboni, K. and P.B. Stark, 2019. Election Integrity and Electronic Voting Machines in 2018 Georgia, *Proceedings of E-Vote ID 2019. Lecture Notes in Computer Science, 11759*, R. Krimmer, M. Volkamer, V. Cortier, B. Beckert, R. Küsters, U. Serdült and D. Duenas-Cid (Eds.) Springer Nature, Switzerland.

there was a manual recount of 2.9 million hand-marked paper ballots cast in the 2008 Minnesota gubernatorial election. Of those 2.9 million ballots, between 99.95% and 99.99% were unambiguously marked.²⁸ A risk-limiting audit can rigorously account for hand-made marks that are not machine readable and/or are genuinely ambiguous, but there is no way to protect against the possibility that machine-made marks are incorrect, because they obscure all evidence of voter intent. Trading the trustworthiness of the entire paper trail to save the labor of manually adjudicating some marks that are not machine-readable—but are clear to human readers—is a Faustian bargain.

46. Dr. Gilbert claims that hand-marked paper ballots are not strongly software independent, because they can be tampered with. Gilbert declaration, at 30. Physically tampering with ballots is not a change to the voting system software: it has nothing to do with software independence or strong software independence. Securely curated hand-marked paper ballots are, in fact, the canonical example of a strongly software independent voting system. Software independence and strong software independence were invented to capture key security properties of properly curated hand-marked paper ballots.

47. He claims that the 2018 de Millo et al. study of whether voters check BMD printout is flawed because it did not study whether voters check hand-marked paper ballots. Gilbert declaration, at 31. He missed the point: there is no way that hacking, misconfiguration, or bugs can cause hand-marked paper ballots to be mismarked. Whether voters check their own work us up to them, but essentially every voter must accurately check BMD output or hacking, misconfiguration, or bugs can alter election outcomes. See paragraphs 14–16, *supra*.

²⁸ Appel et al., 2019.

48. Dr. Gilbert makes blanket statements about the accessibility of BMDs, including systems he has not inspected. Gilbert declaration, at 19ff. I understand that the accessibility of BMDs varies widely, and that a number of current BMD systems have failed multiple states' certification for lack of accessibility. See note 20, *supra*.
49. Dr. Gilbert writes, "If individuals with disabilities vote one way and everyone else votes a different way, this provides fertile ground for an attack. When an attacker knows the specific limitation of the population using a certain system, it is easier for that attacker to tailor an attack without being detected." Gilbert declaration, at 21. In fact, attacks on vulnerable populations are *facilitated* by universal-use BMDs: BMDs know how long the voter takes to vote, whether the voter increases the font size, whether the voter uses the audio interface, whether the voter uses a sip-and-puff device, whether the voter uses a foreign-language ballot, whether the voter reviews and revises selections, whether the voter skips contests, etc., so all those variables can be used by a hacker to target attacks against older voters, voters with cognitive disabilities, voters with physical disabilities, voters with visual disabilities, voters who are not native English speakers, *et al.*²⁹ Reducing the number of voters who use BMDs decreases the "attack surface" (there are fewer machines), reduces the number of votes that can be altered, and makes attacking BMDs less attractive, because fewer votes are vulnerable.
50. Dr. Gilbert implies that ballot design problems only occur with paper ballots. Gilbert declaration, at 30, 31. But BMD screens (and BMD printout) have the same issues.

²⁹ Stark, P.B., 2019.

Design always matters, whether the options are displayed on a screen, by audio, or on paper. Indeed, Gilbert’s own research supports this.³⁰

51. He claims that “[touchscreen miscalibrations] are exceedingly rare in modern touchscreen BMDs unlike older DRE touchscreen machines.” Gilbert declaration, at 32. This assumes that the equipment will function as intended, while the threat model must include the possibility of malicious hacking, misconfiguration, negligence, and interference.

52. For instance, a brand-new ES&S ExpressVote XL BMD system in Northampton, PA, was grossly miscalibrated in an election last month—to the point that voter instructions “received thousands of votes.” See note 19, *supra*.

53. Deliberately miscalibrating a touchscreen to cause a BMD to record votes incorrectly is simple: I personally performed exactly that hack at Def Con this summer. In about 30 seconds, I was able to re-calibrate a touchscreen voting device so that it registered votes for the wrong candidate.³¹

54. Dr. Gilbert asserts “In essence, a BMD is nothing more than an ink pen—but one that can avoid ambiguous marks that belie voter intent.” Gilbert declaration, at 30. In fact, a BMD is a *hackable* pen that leaves no reliable evidence of voter intent. See paragraphs 24, 25, 40, 45, *supra*.

³⁰ Gilbert et al., 2013.

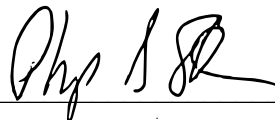
³¹ For an example of voting machine screen miscalibration altering votes “in the wild,” see <https://www.jconline.com/story/news/2019/11/05/faulty-machines-again-blamed-switching-votes-greater-lafayette-races/4163625002/> (last visited 16 December 2019)

MISCELLANY

55. Plaintiffs mention my service on the EAC Board of Advisors in conjunction with the fact that no systems have been certified to VVSG 1.1 or VVSG 2.0. I do not understand the point they are trying to make. The EAC has been very slow to adopt new standards, despite more than a decade of evidence of problems and gaps in the current standard. Many systems have been certified under VVSG 1.0, but not all the systems are equally good, as measured by trustworthiness, reliability, usability, auditability, cost, and other factors. Auditability and software independence were not even recognized as important criteria until VVSG 2.0. As a member of the EAC Advisory board and its Cybersecurity Subcommittee, I have proposed resolutions regarding a several aspects of voting systems that are crucial to provide evidence that reported outcomes are correct, to ensure that the paper trail is trustworthy, and to enable efficient, effective audits. There are a number of commercial systems certified under VVSG 1.0 that accomplish those goals. The universal-use BMD system Georgia chose to deploy does not.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, December 16, 2019.



Philip B. Stark