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

DONNA CURLING, et al.	)	
Plaintiff,	)	
vs.	)	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**
BRIAN P. KEMP, et al.	)	
Defendant.	)	

SECOND SUPPLEMENTAL DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my statements of September 9, 2018, and September 30, 2018. I stand by everything in the previous declarations.
2. I understand that the State of Georgia proposes to deploy ballot-marking devices (BMDs) for all in-person voters. In my opinion, this will do little to improve election integrity in Georgia: BMDs are essentially as vulnerable as the DRE machines they would replace, despite the fact that BMDs generate a "voter-verifiable" paper trail. I shall explain why.
3. I understand that Defendants argue that a BMD-based system is auditable, and that therefore BMD-based voting systems are acceptable. The premise is misleading and the conclusion is false.
4. Every system is auditable—to some extent. The question is not whether a BMD-based system can be audited in some sense. The question is what audits of BMDs can

accomplish, and in particular, whether they can reliably detect whether software bugs, errors, or hacking altered the reported election results. Audits of BMDs cannot.

5. This is in part because BMDs make the paper audit trail vulnerable to malfunctions. Bugs, misconfiguration, or malicious hacking can cause the BMD to print something other than the selections the voter made on the touchscreen or accessible interface. Hand-marked paper ballots do not have that vulnerability.
6. Audits of BMDs cannot reliably detect whether malfunctioning BMDs corrupted the paper trail. (I use the term *malfunction* generically to include problems due to bugs, configuration errors, and hacking.) This is true even if the malfunctions were severe enough to cause losing candidates to appear to win.
7. If an audit or inspection of a BMD happens to discover a malfunction, there is in general no way to tell whether the malfunction altered electoral outcomes, nor any way to determine the correct electoral outcomes. As a result, voting systems based on BMDs are not *strongly software independent*.[1]

---

[1] "Strong software independence" was defined by Rivest, Ronald L., and J. Wack, 2006. On the notion of "software-independence" in voting systems. https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf (last visited 20 October 2019). A voting system is strongly software independent "if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome, and moreover, a detected change or error in an election outcome (due to change or error in the software) can be corrected without re-running the election." Strong software independence is extremely desirable. The draft of version 2.0 of the Voluntary Voting System Guidelines (VVSG 2.0) requires software independence. Draft Voluntary Voting System Guidelines, version 8, 19 September 2019. https://www.eac.gov/assets/1/6/VVSGv_2_0_Scope-Structure(DRAFTv_8).pdf (last retrieved 21 October 2019). Systems based on optically scanning hand-marked paper ballots (with reliable chain of custody of the ballots) are strongly software independent, because inspecting the hand-marked ballots allows an auditor to determine whether malfunctions altered the outcome, and a full manual tabulation from the paper ballots can determine who really won, without having to re-run the election. A risk-limiting audit of an election conducted using hand-marked paper ballots can guarantee a large chance of correcting

8. Only voters are in a position to catch some kinds of BMD malfunction. There is no other mechanism. No feasible amount of parallel or "live" testing or auditing can offer a reasonable chance of catching outcome-changing errors.[2]
9. Even if the vast majority of voters caught and corrected errors in their printout, outcomes as reflected in the BMD paper trail could be wrong, because some contests are decided by small margins.[3]
10. Even if voters notify pollworkers of problems, the way elections are conducted in Georgia (and the rest of the U.S.), there is no mechanism to translate that into remedial action beyond giving voters who complain another chance to mark a ballot. That is partly because voters who observe a problem get no evidence they can show to anyone else to demonstrate that there was a problem. Showing a pollworker or election official the BMD printout does not prove anything: it is the voter's word against the BMD output.[4]
11. Research shows that relatively few voters do check, and they are not good at it.[5]
12. If pollworkers and election officials take voter complaints of BMD malfunctions seriously, their only recourse is to hold a new election. That would make the whole election system vulnerable to crying "wolf."[6]

---

the outcome if it is wrong. In contrast, because BMD printout cannot be trusted to reflect voters' selections, auditors can only determine whether the BMD printout was tabulated accurately, not whether the election outcome is correct, nor can auditors determine the correct outcome.

[2] See 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).

[3] Stark, *op. cit.,* and 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).

[4] Appel et al., *op. cit.*

[5] DeMillo, R., R. Kadel, and M. Marks. 2018. What Voters Are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters' Memories of Their Ballots, SSRN https://ssrn.com/abstract=3292208 (last visited 20 October 2019).

[6] Stark, *op. cit.,* Appel et al., *op. cit.*

13. For the reasons above, the reliance on BMDs in elections should be kept to a minimum. With luck, there will soon be more accessible, meaningfully auditable technologies—technologies that support "evidence-based elections,"[7] as recommended by the most recent draft of Version 2.0 of the U.S. Voluntary Voting System Guidelines.[8] Evidence-based elections are not possible if a noticeable percentage of ballots are marked using BMDs.
14. Unless the State of Georgia adopts rigorous post-election audits, including "compliance audits"[9] and risk-limiting audits (RLAs), using a voting system with a paper trail will not improve the trustworthiness of Georgia's elections at all.
15. I drafted most of the language defining and explaining RLAs in Georgia's Act 24 (2019-HB316) §21-2-498 (a)-(d). However, Act 24 does not require routine RLAs, only a pilot, which is not required until late 2021.
16. The audit requirements under HB 316 are seriously deficient. An audit could satisfy HB 316 and yet have no of discovering or correcting errors, even outcome-changing errors.
17. For instance, HB 316 does not require audits and recounts to be based on the human-readable marks on the paper trail. But a malfunctioning BMD could print barcodes that

---

[7] Stark, P.B., and D.A. Wagner, 2012. Evidence-Based Elections. *IEEE Security and Privacy, 10*, 33-41. DOI: 10.1109/MSP.2012.62. Evidence-based elections require election officials to produce convincing evidence that the reported winner(s) really won. That is not possible if a noticeable fraction of ballots are marked using BMDs.

[8] See Principle 9, "Auditable," in Draft Voluntary Voting System Guidelines, version 8, 19 September 2019. https://www.eac.gov/assets/1/6/VVSGv_2_0_Scope-Structure(DRAFTv_8).pdf (last retrieved 21 October 2019).

[9] Stark and Wagner, op. cit.; Stark, P.B., 2018. An Introduction to Risk-Limiting Audits and Evidence-Based Elections, Prepared for the California Little Hoover Commission, https://www.stat.berkeley.edu/~stark/Preprints/lhc18.pdf (last retrieved 21 October 2019).

do not match the human-readable marks.[10] An audit based on the barcodes cannot possibly detect that.

18. HB 316 does not require audits to take any remedial action if they uncover errors in the electronic tally. Such "toothless" audits do little to ensure election integrity.
19. HB 316 does not require any auditing until November 2020. The presidential primary elections will take place sooner. Absent any auditing, the primaries will be vulnerable to outcome-changing errors and malfunctions that would have a large chance of being caught and corrected by a RLA.

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, October 22, 2019.

_____

Philip B. Stark

[10] A BMD can also print human-readable marks and barcodes that do not match what the voter saw on the touchscreen or heard through the audio interface.