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

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

EXPERT REPORT OF ANDREW W. APPEL

June 28, 2021

Exhibit
0003

TABLE OF CONTENTS

I. Qualifications

1. My name is Andrew W. Appel.

2. My background, qualifications, and professional affiliations are set forth in my curriculum vitae, which is attached as Exhibit A. I have over 40 years' experience in computer science, and 17 years' experience studying voting machines and elections.

3. I am the Eugene Higgins Professor of Computer Science at Princeton University, where I have been on the faculty since 1986 and served as Department Chair from 2009-2015. I have also served as Director of Undergraduate Studies, Director of Graduate Studies, and Associate Chair in that department. I have served as Editor in Chief of ACM Transactions on Programming Languages and Systems, the leading journal in my field. In 1998 I was elected a Fellow of the Association for Computing Machinery, the leading scientific and professional society in Computer Science.

4. I received an A.B. (1981) from Princeton University *summa cum laude* in Physics, and a PhD (1985) from Carnegie Mellon University in Computer Science.

5. I have taught undergraduate and graduate courses at Princeton University in programming, programming languages, software engineering, election machinery, software verification, and formal methods.

6. I have testified on election technology before the U.S. House of Representatives (subcommittee on information technology, 2016), the New Jersey legislature (several committees, on several occasions 2005-2018), the New York State Board of Elections (2019), the Freeholders of Mercer County (2017 and 2019) and Essex County (2019).

7. I have published over 100 scientific articles and books, including many papers on computer security and several papers on voting machines, election technology, and election audits.

8. I have served as a peer-review referee for the Usenix Electronic Voting Technology workshop.

9. I was appointed by the National Academies of Science, Engineering, and Medicine (NASEM) to a Consensus Study Committee 2017-2018, leading to my coauthorship of the peer-reviewed NASEM report, *Securing the Vote: Protecting American Democracy,* 2018.

10. I testified as an expert witness (Computer Science) in *New York v. Microsoft* (Civil Action No. 98-1233 (CKK) in U.S. District Court for D.C.); *Universal Studios v. Reimerdes* (00 Civ. 0277 (LAK), U.S. District Court for S.D.N.Y.); and *Gusciora v. Corzine* (MER-L-2691-04, Superior Court of New Jersey).

II. Assignment

11. I have been asked by counsel for the Curling Plaintiffs to serve as an expert in computer science, cybersecurity, election systems, and voting machine security. I may also respond to expert reports submitted by Defendants if needed.

12. I have not been asked to perform a forensic cybersecurity examination of any specific voting machine. I understand that the Plaintiffs have engaged one or more other experts to do that.

III. Materials Considered

13. Consensus Study Report of the National Academies of Sciences, Engineering, and Medicine, entitled *Securing the Vote: Protecting American Democracy* (2018). The National Academies selected an expert committee of computer scientists, statisticians, law professors, social scientists, and experienced election administrators. The committee met for 6 two-day meetings over 18 months, at which it heard testimony from other experts and other election administrators. The committee was charged with writing a report that reflected the clear scientific consensus. The National Academies had the committee’s report peer-reviewed before publishing it.

14. Richard DeMillo, Robert Kadel, and Marilyn Marks. What Voters are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters' Memories

of Their Ballots (November 23, 2018). ssrn.com/abstract=3292208

15. Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman. Can voters detect malicious manipulation of ballot marking devices? In *41st IEEE Symposium on Security and Privacy,* pp 679-694, 2020.

16. Andrew W. Appel, Richard A. DeMillo, and Philip B. Stark. Ballot-marking devices cannot assure the will of the voters. *Election Law Journal,* vol. 19 no. 3, pp. 432-450, September 2020.

17. Juan Gilbert. Can voters detect ballot manipulations with a transparent voting machine?, seminar presentation (video) at Princeton University, citp.princeton.edu/event/gilbert, March 2021.

18. Verified Voting Foundation Board of Directors (Barbara Simons, PhD, David L. Dill, PhD, Joseph Lorenzo Hall, PhD, David Jefferson, PhD, Ronald L. Rivest, PhD, Kevin Shelley, JD), Statement on Ballot Marking Devices and Risk Limiting Audits, https://verifiedvoting.org/statement-on-ballot-marking-devices-and-risk-limiting-audits/, December 2019.

19. CVE List, cve.mitre.org/cve, consulted April and June 2021. CVE® is a list of publicly disclosed cybersecurity vulnerabilities, maintained by the MITRE Corporation under contract to the Department of Homeland Security.

x

IV. Summary of Opinions

20. It is a clear scientific consensus that any computer-based voting machine can be “hacked,” in the sense that an unauthorized person can install fraudulent software that misrepresents votes and tabulations.

21. It is a clear scientific consensus that the only practical solution to this problem (that is secure enough for use in public elections) is to mark votes on voter-verified paper ballots that can be recounted or audited by hand, in case the computers have (through fraud or inadvertent misconfiguration) counted the votes incorrectly.

22. There is clear evidence, and a growing scientific consensus, that paper ballots marked by touchscreen ballot-marking devices (BMDs) are not *voter-verified* in a strong enough sense to secure elections, and there is no known way of remedying the problem—other than to abandon BMDs except for those voters who cannot mark a paper ballot with a pen.

23. Therefore, the election system recently adopted by Georgia, in which all voters in the polling place mark their ballots by touchscreen BMDs, is inherently

not secure enough for use in public elections in today's environment of advanced persistent threats and computer failures.

24. Other components of the election system recently adopted by Georgia, including optical scanners that are capable of reading hand-marked paper ballots, can be secure enough for use in public elections if properly secured, maintained, and operated.

25. Georgia elections could be rendered sufficiently secure by limiting the use of BMDs (such as the Dominion ICX touchscreens) to those voters who cannot mark a paper ballot by hand.

V. Background

26. A voting machine—whether a direct-recording electronic (DRE) touchscreen, a ballot-marking device (BMD), a precinct-count optical scanner (PCOS), a central-count optical scanner (CCOS), or some hybrid of those—contains a computer that directs its operations. This was not true of mechanical lever machines (outlawed by Congress in 2002) or punch-card voting booths (also outlawed in 2002) but is true of today's technology.

27. The software (computer program) running on this computer interprets the inputs from the voter as *votes* for one candidate or another, and then that same or another computer tabulates, prints, or transmits those votes. It is straightforward to

write a fraudulent program that deliberately misinterprets the voters' inputs as votes for a candidate that the voter did not intend; (depending on what kind of voting machine it is) that deliberately mistabulates or misprints votes; or that deliberately transmits votes other than those the voter intended. If a malicious actor can manage to install such a fraudulent program in a voting machine, then he can disenfranchise individual voters by altering their intended votes, and even alter the outcome of elections.

28. Computers are *designed* to allow the installation of new software—that has been the essence of a computer since 1950. There are many ways in which software can be installed in a computer such as a voting machine:

a. In the factory, by insiders or by hackers who have penetrated the factory's computer network.

b. Through the standard "firmware upgrade" process, by insiders or by hackers who have penetrated the factory's computer network, or by hackers who have penetrated a state or county computer network. Any maker of voting machines needs to "future-proof" the machines they sell by providing some mechanism to update the software. For example, if a jurisdiction might in the future adopt some innovation such as "vote for 3 candidates" or "instant runoff," a new program may need to be installed that can handle such elections. Typically, this is done by writing the firmware-upgrade files to a removable media (memory card or USB thumbdrive), and inserting that media into a port in the voting machine. But fraudulent firmware upgrades can also be installed through the same pathway.

c. Through other pathways, by exploiting "code injection vulnerabilities" in the software of the voting machine. I will explain this below.

29. Some of the pathways for installing fraudulent software in voting machines do not require the voting machine to be connected to a network, do not require the attacker to have physical access (or even proximity) to the voting machines, and permit a single remote attacker to subvert thousands of voting machines. This was first demonstrated (for voting machines) by computer scientists in 2006[1], using underlying principles that had been known since the 1970s.

30. Voting machine makers—like other makers of computers, software, and operating systems—attempt to prevent the installation of unauthorized software using a variety of protection mechanisms. This is a good thing. But it is extremely difficult to make software perfectly secure. Software routinely contains bugs (design and implementation mistakes); some bugs are *exploitable security*

[1] Feldman, Ariel J., J. Alex Halderman, and Edward W. Felten. "Security Analysis of the Diebold AccuVote-TS Voting Machine." In *2007 USENIX/ACCURATE Electronic Voting Technology Workshop,* August 2007.

vulnerabilities, in the sense that an attacker can use the bug as a means of installing fraudulent software.

31. For example, my review of the CVE database (Common Enumeration of Vulnerabilities) maintained by the MITRE Corporation and sponsored by the Department of Homeland Security, shows that the widely used Android operating system has about 103 new serious exploitable vulnerabilities every year, and the iOS operating system (for iPhones) has about 25 per year (2018-2020). In each of those years, between 4 and 75 serious vulnerabilities were also discovered in the Windows 10 operating system. These operating systems are maintained by Google, Apple, and Microsoft respectively, three of the most capable and well-resourced engineering firms in the world; and they cannot entirely prevent pathways in their products for the installation of fraudulent software. Many of those bugs (causing serious security vulnerabilities) lay in the software for years before being discovered by the "good guys" who publish them in CVE, and were (therefore) exploitable by any "bad guys" who were able to find them. Other such bugs not yet discovered by "good guys" continue to be exploitable by "bad guys".

32. Voting machines are not inherently different, and in fact share some of the same software components with Android, iOS, or Windows.

33. Modern computer systems (including voting machines) have many layers of

software, and an insecurity in any one of those layers can compromise the security of all the layers above it.[2] That is, the *application* (vote-interpreting or vote-counting software) runs in a *runtime system*, which runs atop an *operating system*, which relies on *device drivers* to interact with disk drives and external input/output ports; the operating system is installed by a *BIOS* and/or *management engine,* all of which is interpreted by a CPU that may have *writable microcode.* Each of these italicized components is responsible for installing or interpreting the prior-mentioned upper-layer components, so that if one component is compromised by an attacker, that component can easily substitute fraudulent upper layers. For example, if the operating system is subverted, then the legitimate vote-counting application may not be the one that actually gets run on election day; the hacked operating system may substitute a different, hidden, fraudulent vote-counting application program.

34. It is a clear scientific consensus that paperless computerized voting machines are reprogrammable by malicious actors, and are subject to misconfigurations and mistakes by nonmalicious actors; and are therefore not securable by any known or envisioned technology; and are therefore inappropriate

[2] See pages 89-90 of: Securing the Vote: Protecting American Democracy, by National Academies of Science, Engineering, and Medicine (Lee C. Bollinger, Michael A. McRobbie, Andrew W. Appel, Josh Benaloh, Karen Cook, Dana DeBeauvoir, Moon Duchin, Juan E. Gilbert, Susan L. Graham, Neal Kelley, Kevin J. Kennedy, Nathaniel Persily, Ronald L. Rivest, Charles Stewart III), https://doi.org/10.17226/25120, September 2018.

for use in public elections. This consensus is clearly stated in, for example, the Consensus Study Report of the National Academies of Sciences, Engineering, and Medicine, entitled *Securing the Vote: Protecting American Democracy* (2018).

35. Also in the scientific consensus of 2018 reflected in the National Academies' report is that: "Elections should be conducted with human-readable paper ballots" and that "States should mandate risk-limiting audits [of those paper ballots] prior to the certification of election results."

36. Computer scientists and cybersecurity experts who understand and explain the cyber-insecurities of computer-based voting machines are *not* saying, "Voting machines X, Y, and Z are imperfectly secure, so don't use them;" they are *not* saying "wait until perfectly secure machines are available." Instead the experts are saying, computer systems are *inherently* susceptible to cybersecurity risks; they can be very helpful in elections, but are appropriate *only* if the election can be organized in such a way that the result can be trustworthy even with the use of imperfectly securable computers."

37. As I will explain, Georgia's current system of elections using BMDs is *not* sufficiently trustworthy in that sense.

Terminology: Voter verifiable *versus* voter verified paper ballots

38. In the presidential election of 2000, it became widely recognized[3] that punch-card voting systems were severely flawed; those systems were outlawed by the Help America Vote Act of 2002, which also provided funds for states to adopt other voting systems. Many states had already been using optical-scan voting systems (which do not have the same flaws as punch cards) and continued to use them; other states adopted DREs—direct recording electronic voting machines, that use a touchscreen or screen+buttons interface to record votes without printing them on paper. Computer scientists immediately recognized the inherent flaw in DRE voting machines—whoever gets to install the computer program gets to decide the vote count—and communicated with policymakers at the county, state, and national level. Since 2007, most states that had adopted DREs have discarded them in favor of optical-scan voting systems, and since 2007 no state has adopted paperless DREs. I believe the reason the states have done that is because of the inherent insecurity of DREs as explained by computer scientists.

39. Computer scientists have recommended since 2001, and states largely adopted 2004-2012, the principle of the *voter-verifiable paper ballot.* That means, since one cannot trust a computerized voting machine to have the correct

[3] Flaws in punch-card voting systems were already well understood and explained by some experts. *see* Saltman, Roy, *The History and Politics of Voting Technology,* Palgrave McMillan 2006.

(unhacked) software installed on election day, there must be a paper ballot that the voter can see, that the voter can *verify* contains votes for the candidates the voter intended; and that same paper ballot can be recounted by hand, by a person who can see the same votes that the voter verified.

40. In this report, I will carefully distinguish between the notion of *voter-verifiable paper ballot* and *voter-verified paper ballot.* The former is a paper ballot that the voter could, in principle, inspect and verify that it contains the right votes. The latter is a paper ballot that we have good reason to believe that the voter *has* verified to make sure it contains the right votes. This distinction was not widely understood or analyzed, even by scientists, until recent years.

41. Some people have reasoned, "since the computers cannot be fully trusted, we should not use them to count votes, we should count votes only by hand." Hand counting works quickly and accurately in countries with unitary parliamentary democracies where there is usually only one contest on the ballot. But the complexity of U.S. elections—the sheer number of different contests on the ballot—makes it difficult to do hand counting quickly and accurately.

42. Most voting machines are highly accurate most of the time, when used properly, when they have not been hacked, and when there has not been a mistake in configuration or a mechanical problem (e.g., miscalibrated touchscreen, dust

buildup in sensors, etc.). Therefore it is reasonable to use optical-scan voting machines, provided one audits for errors or hacks using the voter verifiable paper ballot and the machines are configured properly to reliably capture votes.

43. One form of voter-verifiable paper ballot is a hand-marked paper ballot, counted by hand or counted by an optical-scan voting machine (either at the polling place, PCOS, or at a central location, CCOS). Computer scientists have generally endorsed hand-marked paper ballots (HMPB) with optical scan since about 2003 (when attention was first focused on the issue).

44. Another form of voter-verifiable paper ballot, proposed in approximately 2000, was the VVPAT, *voter-verifiable paper audit trail,* an attachment to a DRE voting system that would print out a record of the voter's choices that the voter could see and verify; the VVPAT record would then drop into a sealed ballot box for use in later recounts. Computer scientists (including myself) generally endorsed this concept in the period 2003-2008, but it was later found to have fundamental flaws (as I will explain below) and the current consensus of scientists is that this is not a secure method of voting. Few states still use DRE+VVPAT machines (except to accommodate voters with disabilities who cannot mark a paper ballot by hand).

45. Another form of voter-verifiable paper ballot is a ballot produced by a *ballot*

marking device (BMD), such as the Dominion ICX that is at issue in this case. Many computer scientists endorsed this concept in the period 2003-2018, but it was later found to have fundamental flaws (as I will explain below) and the current consensus of scientists is that this is not a secure method of voting.

46. Another form of voter-verifiable paper ballot is a ballot produced by a *hybrid BMD,* such as the ES&S ExpressVote, that can both print a ballot and scan that ballot in the same paper path. Such machines are inherently insecure, but they are not at issue in this case and I will not discuss them further.

47. I have not examined the particular voting machine at issue in this case, the Dominion ICX. I understand that another expert is examining that specific machine for possible bugs, insecurities, and vulnerabilities. If that expert finds specific insecurities and vulnerabilities, it will be entirely unsurprising, because of the inherent nature of modern computer-system designs. If specific insecurities and vulnerabilities are found in the Dominion ICX, then they should be remedied. *But that would not eliminate the possibility, indeed the* ***probability****,* that there are more insecurities and vulnerabilities yet to be found.

VI. Analysis

48. In the Background section above, I discussed the scientific consensus that had entirely solidified by 2010, that was reported in the National Academies'

report in 2018, and that I understand is not contested by any party in this case: computer-based voting machines can be compromised by the installation of unauthorized software that may deliberately miscount votes, and therefore a voter-verifiable paper ballot is required, so that a recount of paper ballots will recount the same marks that the voters actually saw and accepted (to the extent they reviewed the paper ballot before submitting it for tabulation).

49. In this section I will discuss a scientific consensus regarding ballot-marking devices (BMDs) that solidified in 2019-2020.

50. First I will review the way in which Georgia uses BMDs in the polling place. Each voter, upon having identity and registration verified and upon signing the pollbook, is directed to a touchscreen BMD, the Dominion ICX. The voter uses the touchscreen to select choices in every contest. The voter may use a review screen on the BMD to proofread the choices.

51. Then the BMD prints out a paper ballot that lists (in plain text) the voter's choice of candidate in each contest (assuming it prints the selections correctly)[4]. The paper ballot also has a QR code, a two-dimensional barcode that encodes all these choices. I reproduce an image of such a paper ballot as Exhibit B.

[4] In the case of referendum questions, the ballot reflects a choice that is not a "candidate" per se. In the remainder of this discussion, without loss of generality, I will refer to these choices as "candidates."

52. The voter may review the paper-ballot to try to ensure the plain-text selections are correct, but the voter is unable to know what selections are reflected in the QR code.

53. The voter then brings the ballot paper to a precinct-count optical scanner (PCOS), and feeds it in. The scanner reads the QR code and tabulates the votes encoded there. The scanner drops the paper ballot into a ballot box; the paper ballots are saved for possible use in recounts and audits.

54. I will explain the (flawed) theory by which this method of voting would be appropriate. In this theory, we assume that either the BMD (Dominion ICX) or the optical scanner (Dominion ICP) may be hacked, that is, a would-be election thief installs fraudulent software that misprints or miscounts votes. If the BMD were hacked, then on the review screen (prior to printing) it would show the voter the choices that the voter actually made, but it could print votes onto the paper (in plain text) that were different from the voter's choices, or it could encode votes into the QR code on the paper different from the voter's choices, or both. In either case, these fraudulently printed votes would differ from the voter's actual selections.

55. For the sake of discussion, suppose the voter has chosen candidate Smith on the touchscreen, and a BMD running the legitimate correct software would print

Smith in plain text onto the paper ballot and encode Smith into the QR code. A hacked BMD could print candidate Jones in plain text, or encode Jones into the QR code, or both. Whichever candidate is encoded into the QR code is the one that will be tabulated by the optical scanner.

56. In this theory, the voter is expected to review the printed ballot, and if a plain-text printed candidate choice is incorrect, the voter is expected to notify a pollworker that there is a problem, and the pollworker is expected to tell the voter that she can void this paper ballot and start over at the BMD.

57. In this theory, not every single voter must meticulously check every single choice on the printed paper ballot; if any significant fraction of voters checks carefully, and if the BMDs are systematically cheating, then a significant number of voters will inform the pollworkers, and there will be some remedy to correct the problem.

58. In this theory, because of the expected behavior (of voters and election workers) described in the previous two paragraphs, the fraudster dares not hack the BMDs to misprint the plaintext candidate choices. So the plaintext candidate names on paper ballots record the voter’s true intent. The theory holds that any recount of the ballots will be by human inspection of the human-readable portion of the paper ballot, and will therefore correctly obtain the result preferred by a

majority of the voters.

59. In this theory, a risk-limiting audit or a recount of the paper ballots will catch and remedy the fraud. The BMD may be hacked to encode fraudulent choices into the QR code, e.g., Jones. In such a case the voter cannot notice the fraud. The optical scanner will tabulate a vote for Jones. The election outcome reported by the optical scanners (in aggregate) will contain more votes for Jones than the voters marked on the touchscreens, and fewer for Smith. But this theory holds that a risk-limiting audit or a recount of the paper ballots will ignore the QR codes and read the human-readable portion of the paper ballots; the true election outcome will be obtained; the fraud will not succeed. The theory further holds that even if the BMD is not hacked and runs authorized correct software, a risk-limiting audit or a recount of the paper ballots still will detect and correct the fraud. For example, the PCOS (precinct-count optical scanner) may be hacked such that if the QR code encodes Smith the PCOS may tabulate a vote for Jones. In this theory, this sort of fraud also would be detected by a risk-limiting audit or recount.

60. This (flawed) theory was generally accepted 2003-2010 by most computer scientists who studied election cybersecurity, including myself; and it was accepted by many computer scientists even until 2018. New experimental evidence in 2018 and 2019, followed by new scientific analysis in 2018 and 2019, has refuted certain

key premises of this theory, and it is no longer generally accepted.

61. This theory, that would justify the use of BMDs for all voters, has two key flaws:

a. Flaw 1: The assumption that "The voter is expected to review the printed ballot, and if a plaintext printed candidate choice is incorrect, the voter is expected to notify a pollworker that there is a problem, and the pollworker is expected to tell the voter that she can void this paper ballot and start over at the BMD."

b. Flaw 2: The assumption that if any significant fraction of voters checks carefully, and if the BMDs are systematically cheating, and if a significant number of voters will inform the pollworkers, that "there will be some remedy to correct the problem."

62. A paper published in November 2018[5] reported on observations of real voters, using real BMDs, in two real polling places in Tennessee, during an August 2018 primary election. In the polling places, voters marked their ballots on touchscreen BMDs, which printed out paper ballot cards. Voters carried their ballot cards from the BMD to the PCOS (precinct-count optical scanner). The

[5] 15. Richard DeMillo, Robert Kadel, and Marilyn Marks. What Voters are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters' Memories of Their Ballots (November 23, 2018). ssrn.com/abstract=3292208

experimental observer, stood in a place where the public was permitted, far enough away to preserve the privacy of the secret ballot, close enough to observe voters' behavior.

63. Only 53% of the voters even reviewed their printed ballot at all; 47% did not review the ballot for even one second. The voters who did review their ballot spent an average of 3.9 seconds doing so. There were 18 contests on the ballot, so that is (on average) less than ¼ of a second review per contest. This casts strong doubt on the assumption that "the voter will review the printed ballot, and if there is an error on it, will notify a pollworker."

64. A study released in 2019 (and published in peer-reviewed form in 2020)[6] examined the behavior of real voters using real BMDs in a simulated polling place, not in a real election. The researchers performed a controlled experiment: they set up BMDs in a public library in Michigan, and asked library patrons to participate in "a study about the usability of a new type of voting machine." The BMDs were specially hacked to print, in one contest per paper ballot, a different candidate than the voter had selected. Only 7% of the voters reported the error to a poll worker, and only 8% reported the error on an exit survey. This casts strong doubt on the

[6] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman. Can voters detect malicious manipulation of ballot marking devices? In 41st IEEE Symposium on Security and Privacy, pp 679-694, 2020.

assumption that "the voter will review the printed ballot, and if there is an error on it, will notify a pollworker."

65. A paper released in 2019 (and published in peer-reviewed form in 2020),[7] of which I was a coauthor, analyzed the consequences of that experimental evidence, with particular focus on the assumption that "if a significant number of voters will inform the pollworkers that their ballots were printed incorrectly, there will be some remedy to correct the problem."

66. I will explain our analysis in that paper, as it bears directly on the question of whether elections can securely be conducted on BMDs, in Georgia or elsewhere.

67. Suppose a hacker has installed fraudulent software in a BMD that in one contest, some small fraction of the time (e.g., 1/100) prints candidate Jones onto the paper instead of candidate Smith. Suppose only a small fraction of the voters (e.g., 7/100) inspect their ballots carefully enough to notice such an error. Then only the product of those fractions (e.g., 7/10000 or approximately 1 in 1425) will notify a pollworker of a problem with their ballot. That may be only one or two voters per polling place.

68. The pollworkers will (presumably) allow the voters to remake their ballots

[7] Andrew W. Appel, Richard A. DeMillo, and Philip B. Stark. Ballot-marking devices cannot assure the will of the voters. Election Law Journal, vol. 19 no. 3, pp. 432-450, September 2020.

on the BMDs. However, of those 1% of the ballots on which the BMD cheated, 93% will not be corrected. Therefore, the hacker will have succeeded in subtracting 0.93% of the votes from Smith and adding 0.93% of the votes to Jones, a swing of more than 1.8%.

69. Many elections are decided by such small margins. This would have been much more than enough to alter the outcome of several recent elections in Georgia, including the 2020 Presidential election and one of the January 2021 Senate runoff elections.

70. If the hacker had decided to steal a larger fraction of the votes, perhaps 2% or 3%, the analysis would be similar—except that one out of 700 or one out of 475 voters in the polling place might ask to remake their BMD ballots.

71. If Georgia voters were more meticulous than voters in Tennessee or Michigan, so that a slightly larger fraction would carefully inspect their ballots, the analysis would be also be similar, with slightly more voters in the polling place asking to remake their BMD ballots.

72. You might think, "those one or two voters in each polling place *caught the BMD cheating, red-handed.*" It is true, they did. But the voter has no way of proving that to the pollworker or to anyone else, because nobody else saw which candidate the voter indicated on the touchscreen. The pollworker—and maybe

even the voter—likely would simply conclude that the voter was mistaken about what they did on the touchscreen and the printed ballot correctly reflects the voter's selections that actually were made on the BMD.

73. You might think, "but if *several* voters report the same problem, that's evidence that the BMD is cheating." But, unfortunately, a large number of voters would have to make such reports to raise even the suspicion of a problem with the equipment that was altering votes from those selected on the BMD. And even if such suspicion arose, likely the most that would happen is that the particular BMD would be removed from use in that election; other BMDs equally compromised still would be in use in that election. Moreover, if voters were to falsely make such claims in order to cast doubt on the election, and there would be no way to prove that those voters are lying or telling the truth.

74. Suppose, counter to fact, that a few voters *could* prove that the BMD had cheated. Even then, there is no remedy that an election official could apply, other than throwing out the results of the election and calling for a new election. This would be an extraordinary remedy and it is unclear how—and whether—it would even be possible. And again, if only the votes made on that BMD were remedied, that would leave the fraud affecting other votes made on other BMDS undetected and unremediated.

75. In contrast, suppose an optical-scan voting machine had been hacked to cheat. If risk-limiting audits (RLAs) were routinely used, the RLA would be highly likely to detect that there was a problem, and there is a clear way to correct the problem: recount the paper ballots by hand. It would not be necessary to conduct a "do-over" election. Even if RLAs were not used, if *any* evidence were to cast doubt on the accuracy of the voting-machine tabulation, a recount would correct the problem, if any. This is the fundamental difference between BMD hacking and optical-scanner hacking: BMD hacking is not reliably detectable and it is not correctable short of an election do-over; optical-scanner hacking is reliably detectable and it is fully correctable without an election do-over.

76. And finally, suppose in some election the BMDs have not been hacked at all, and are faithfully printing the choices made by voters. But suppose a few hundred voters statewide, distributed among many polling places, report to pollworkers and the media that the BMDs have changed their votes. There will be no way to prove them wrong. These few hundred voters could then cast doubt upon all the election results; and this doubt could not be resolved by doing a recount, for the reasons I have described above. I regret that this scenario has become all too plausible.

Scientific Consensus

77. It is now a scientific consensus that paper ballots marked by touchscreen

ballot-marking devices (BMDs) are not *voter-verified* in a strong enough sense to secure elections, and there is no known way of remedying that problem—other than to abandon BMDs except for those voters who cannot mark a paper ballot with a pen.

78. In December 2019 the Verified Voting Foundation's board of directors released a statement[8] saying, in part,

> "[E]mpirical research thus far shows that few voters using BMDs carefully verify their printed ballots. Moreover, if voters do verify BMD-marked ballots and find what they believe are discrepancies, there is no reliable way to resolve whether the voters made mistakes or the BMDs did. For these and other reasons (such as cost) Verified Voting recommends that the use of BMDs be minimized."

79. Verified Voting is a nonpartisan nonprofit 501(c)(4) corporation founded in 2004 "to promote social welfare through championing reliable and publicly verifiable elections in the U.S."[9] Its board of directors (at the time of issuing this statement) comprised five Ph.D. computer scientists plus the former Secretary of

[8] Verified Voting Foundation Board of Directors (Barbara Simons, PhD, David L. Dill, PhD, Joseph Lorenzo Hall, PhD, David Jefferson, PhD, Ronald L. Rivest, PhD, Kevin Shelley, JD), Statement on Ballot Marking Devices and Risk Limiting Audits, https://verifiedvoting.org/statement-on-ballot-marking-devices-and-risk-limiting-audits/, December 2019.

[9] Articles of Incorporation, https://verifiedvoting.org/wp-content/uploads/2020/07/vvo.articles.pdf

State of California. Its Board of Technical Advisers comprises approximately 18 Ph.D. computer scientists (including me) and 56 other experts in law, elections administration, and cybersecurity.

80. Juan E. Gilbert is the Andrew Banks Family Preeminence Endowed Professor of Computer & Information Science at the University of Florida. He has done substantial research on user interfaces, voting machines, and ballot-marking devices (BMDs). In March 2021 he gave a seminar talk at Princeton University on research he had been conducting since 2019, motivated by the fact that "If the BMD is hacked or misprogrammed so that it prints a different candidate selection than the voter indicated on the touchscreen, the voter is supposed to notice this; this is an essential protection against hacking and programming bugs. Recent studies have shown that, unfortunately, only a small fraction of voters read their paper ballot carefully enough to catch errors. That's a problem, because errors printing the paper ballots cannot be caught by recounts." (quoted from the abstract of his talk)[10]

81. Professor Gilbert has designed his own BMD to try to address the widely-acknowledged fact that voters typically do not verify their votes on BMD-

[10] Juan Gilbert. Can voters detect ballot manipulations with a transparent voting machine?, seminar presentation (video) at Princeton University, citp.princeton.edu/event/gilbert, March 2021.

generated ballots before submitting them for tabulation. His prototype BMD is physically very different from any BMD currently manufactured or sold, including the Dominion ICX at issue in Georgia. His experimental design is meant to improve the rate at which human voters will check their BMD-printed paper ballots for accuracy. His initial user studies (reported in that seminar talk) show a promising improvement. But he says that his BMD is only a research prototype, not a product. And I believe that his motivation to do this research is that he recognizes that all current-model BMDs are not effectively voter-verifiable.

82. Dr. Josh Benaloh is a researcher at Microsoft Research with decades of experience in voting systems and cybersecurity. Ten years ago he was a collaborator in the design of a BMD-based voting system called "Star Vote" which had (in addition) certain other "end-to-end verifiability" features. In June 2021, he (as an employee of Microsoft in a joint announcement with Hart Intercivic, a manufacturer of voting machines) announced a new design in which those same "end-to-end verifiable features" are now usable with *hand-marked paper ballots*, with no need to use BMDs. He did this in recognition of the "growing scientific consensus"[11] that BMDs have the voter verifiability problem that I have described in this report.

[11] Quotation from Josh Benaloh in telephone conversation with Andrew Appel and R.C. Carter, June 2, 2021.

Accommodation for voters with disabilities

83. Some voters are not able to mark a paper ballot with a pen, either because of a vision disability, motor disability, or other disability. Federal law requires, and prudent public policy would suggest, that an "accessible" voting machine be available for the use of such voters. A reasonable technical means to achieve this is through the use of a BMD, equipped with additional interfaces such as audio reading of the ballot choices, large buttons distinguishable by voters with vision impairment, and so on. Such a BMD would print out a paper ballot in the same optical-scan format as for all other voters, marked with the voter's choices (if operating correctly).

84. This is not a perfect solution. First, not all voters with disabilities are able to read and verify a printed paper ballot—though even many blind voters now have smartphone apps or other devices that can read print on paper. Second, just like the voters measured in the experimental studies I have reported on, voters with disabilities may not take the trouble to examine the paper printout and therefore may be vulnerable to hacked BMDs stealing their votes.

85. However, I know of no perfect design for an accessible voting machine, and all other designs for voting machines accessible to voters with disabilities are no better. Therefore, I consider it reasonable to provide BMDs for the use of voters

who cannot easily mark a paper ballot with a pen. However, that is no reason to provide BMDs for the use of all voters, with the consequent election insecurity that I have described in this report.

Conclusion

86. The use of BMDs, by voters who are otherwise able to mark a paper ballot with a pen, is not adequately secure for use in public elections. BMDs can be hacked to steal votes with little likelihood of detection, with no recourse in case of detection (other than entirely discarding an election), and with an additional unnecessary mode of casting doubt on election results even when no hacking may have occurred.

Executed on this 28th day of June, 2021, in Ithaca, New York.

Andrew W. Appel