N.C. STATE BOARD OF ELECTIONS

PETITION FOR RULE-MAKING
(08 N.C.A.C. 15 .0101)

REQUEST FOR EXPEDITED CONSIDERATION
(G.S. §§ 163A-741(a) and 163A-1115; 08 NCAC 04 .0302(a)(7))

I, Lynn Bernstein of Wake County, hereby petition the N.C. State Board of Elections (State Board) as authorized by 08 N.C.A.C. 15 .0101 to adopt the below-described administrative rule regarding the certification of voting systems in North Carolina. Notwithstanding deadlines governing consideration of this Petition, I additionally request expedited review consistent with the State Board’s authority under G.S. §§ 163A-741(a) and 163A-1115; 08 NCAC 04 .0302(a)(7).

The following is submitted in the form required by 08 N.C.A.C. 15 .0101:

(1) the name and address of the person submitting the petition

Lynn Bernstein
421 Wayfield Lane
Cary, NC 27518

(2) a citation to any rule for which an amendment or repeal is requested

The Petition is for a new rule and does not repeal any prior rule. The draft (Section 3, below) suggests an addition to existing 08 NCAC 04 .0302.

(3) a draft of any proposed rule or amended rule

08 NCAC 04 .0302:

(d) Voting systems certified by the State Board must produce paper ballots consistent with the following:
   (1) The ballot must record the voter’s selection by means of a mark;
   (2) The mark must be tabulated as the vote’s selection; and
   (3) The mark must be human-readable.

Nothing in this subsection shall limit the State Board’s certification of voting systems for use by persons with disabilities under the Help America Vote Act of 2002 or other applicable law.
(4) an explanation of why the new rule or amendment or repeal of an existing rule is requested and the effect of the new rule, amendment, or repeal on the procedures of the State Board of Elections

Voters should be able to verify their votes. The General Assembly appears to agree:

The State Board may certify voting systems only if they meet the requirements set forth in this section and only if they generate a paper ballot which provides a backup means of counting the vote that the voter casts. Those voting systems may include optical scan and direct record electronic (DRE) voting systems that produce a paper ballot.

... (5) With respect to DRE voting systems, that the paper ballot generated by the system be viewable by the voter before the vote is cast electronically, and that the system permit the voter to correct any discrepancy between the electronic vote and the paper ballot before the vote is cast.


Vendors are seeking certification of touch-screen systems that record a voter’s selection by displaying the choices onscreen, printing the name of her preferred candidate, and printing a barcode. While evidence in the State Board’s possession shows that voters are unlikely to review their ballot, a vigilant voter will have taken care to review her selections onscreen, print the ballot, and then review the name printed on her ballot. But make no mistake, the barcode is the vote. The tabulator does not detect what was or was not onscreen, and the printed name is not tabulated.

The cautious voter could have done everything right, verifying her selections every step of the way, but the final verification is not a step humans are capable of performing; she must trust that the barcode reflects her choices. She would be unaware of and therefore unable to correct for systematic errors, bugs or hacking that resulted in an incorrect barcode translation of her vote. The process fails to afford the voter her statutory right “to correct any discrepancy,” because any discrepancy would be unknowable since barcodes are not human-readable. (see above).

Materials already provided to the State Board by the League of Women Voters and others during the ongoing certification process make clear what the State Board already knows: Cyber actors have targeted and will continue to target state elections networks and voting systems vendors. The State Board should bear in mind that a system deemed secure today may not be able to be secured over the product’s lifecycle. Cyber actors are creating new ways to infiltrate systems on a daily basis. County boards across North Carolina still use equipment certified more than a decade ago, and the equipment now up
for certification will likely be used far into the future. **Digital voting systems accrue risks, some of which are mitigated by human-readable paper ballots.**

Ballots that are not human-readable may undermine trust in the democratic process leading to the perception that the vote could be compromised. **It is not enough to say that counties perform a hand-eye audit to verify the ballot and tabulation process.** The statutory audit identifies in advance of the election which single contest will be audited and all other races are exempt from the audit. **Elections conducted by tabulating non-human readable marks cannot be confirmed by audits of any kind because the voter is unable to verify that the barcode matches their intent.**

**The proposed rule gives life to statutory guarantees, mitigates vulnerabilities, and better promotes confidence in the elections process.**

Thank you for your consideration.

(5) any other information the person submitting the petition considers relevant.

Attachments:

Stark letter 2.19.pdf  Letter to Subcommittee on Voting Technology  
February 18, 2019  
Ballot-marking devices (BMDs) are not secure election technology

ExpertsLetters.pdf  Experts Letter to SAFE Commission

SSRN-id3292208.pdf  What Voters are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters’ Memories of Their Ballots

SSRN-id3375755.pdf  Ballot-marking devices (BMDs) cannot assure the will of the voters

Lynn Bernstein  07/12/19  
Lynn Bernstein  Date
January 7, 2019

The Honorable Robyn Crittenden
Secretary of State Elect Brad Raffensperger
Rep. Barry Fleming
Members of the SAFE Commission
214 State Capitol
Atlanta, Georgia 30334 (via e-mail)

Dear Secretary Crittenden, Secretary Elect Raffensperger, and SAFE Commission Members:

We write to urge you to follow the advice of election security experts nationwide, including the National Academies of Sciences, the Verified Voting Foundation, Freedomworks, the National Election Defense Coalition, cyber security expert and Commission member Professor Wenke Lee, and the many states that are abandoning vulnerable touchscreen electronic voting machines in favor of hand-marked paper ballots as the best method for recording votes in public elections.

Our strong recommendation is to reject computerized ballot marking devices (BMDs) as an option for Georgia’s voting system, except when needed to accommodate voters with disabilities that prevent them from hand-marking paper ballots. Hand-marked paper ballots, scanned by modern optical scanners and used in conjunction with risk-limiting post-election audits of election results, should be the standard balloting method statewide.

Although they are expensive and complex devices, computerized ballot markers perform a relatively simple function: recording voter intent on a paper ballot. Since there are no objective, quantitative studies of their benefits, acquiring BMDs for widespread use risks burdening Georgia taxpayers with unnecessary costs. Furthermore, BMDs share the pervasive security vulnerabilities found in all electronic voting systems, including the insecure, paperless DREs in current use statewide. These reasons alone should disqualify BMDs from widespread use in Georgia’s elections, especially since there is a better alternative.

Hand-marked paper ballots constitute a safer and less expensive method of casting votes. Hand-marked paper ballots offer better voter verification than can be achieved with a computerized interface. A paper ballot that is indelibly marked by hand and physically secured from the moment of casting is the most reliable record of voter intent. A hand-marked paper ballot is the only kind of record not vulnerable to software errors, configuration errors, or hacking.

The SAFE Commission has heard testimony about voter errors in marking paper ballots and the susceptibility of paper ballots to tampering or theft. No method of balloting is perfect, but vulnerabilities in computerized marking devices, if exploited by hackers or unchecked by bad system designs, raise the specter of large-scale, jurisdiction-wide failures that change election outcomes. For example, with hand-marked paper ballots, voters are responsible only for their own mistakes. On the other hand, voters who use BMDs are responsible not only for
their own mistakes but also for catching and correcting errors or alterations made by a BMD which marks ballots for hundreds of voters. For this reason, well-designed hand-marked paper ballots combined with risk-limiting post-election tabulation audits is the gold standard for ensuring that reported election results accurately reflect the will of the people.

Voter verification of a BMD-market ballot is the principle means of guarding against software errors that alter ballot choices. Many BMDs present a ballot summary card to the voter for verification. The 2018 National Academies of Science, Engineering and Medicine Consensus Report *Securing the Votes: Protecting American Democracy*, which represents the nation’s best scientific understanding of election security and integrity, states: “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.” Although advocates of touchscreen ballot marking devices claim that the human readable text ballot summary cards are “voter verifiable,” the contrary is true: voter verified summary cards that contain errors (whether induced by hacking or by design flaws) are likely to be mistakenly cast, making a valid audit impossible. A post-election audit requires a valid source document, either marked directly by the voter or voter verified. Since voter verification of printed ballot summary cards (the source document) is sporadic and unreliable, elections conducted with most ballot marking devices are unauditable.

While you may have been told that touchscreen systems are more “modern” devices, many of your peers and most election security experts have found this appeal to be based on a mistaken view that the voting public will naively accept new technology as a “step forward.” We are intimately familiar with the hidden costs, risks, and complexity of these new technologies. We can assure you there is objective scientific and technical evidence supporting the accuracy of traditional, easily implemented scanned and audited hand-marked paper ballot systems. We urge you to recommend such a system as the safest, most cost-effective, and transparent way of conducting future elections.

If we can be of help in providing more information, we hope you will feel free to call upon us.

Sincerely,

Dr. Mustaque Ahamad  
Professor of Computer Science,  
Georgia Institute of Technology

Dr. Andrew Appel  
Eugene Higgins Professor of Computer Science  
Princeton University

Dr. David A. Bader, Professor  
Chair, School of Computational Science and Engineering  
College of Computing  
Georgia Institute of Technology

Matthew Bernhard  
University of Michigan  
Verified Voting
Dr. Matt Blaze  
McDevitt Chair in Computer Science and Law  
Georgetown University

Dr. Richard DeMillo  
Charlotte B. and Roger C. Warren Professor of Computing  
Georgia Tech

Dr. Duncan Buell  
NCR Professor of Computer Science and Engineering  
Dept. of Computer Science and Engineering  
University of South Carolina

Dr. Larry Diamond  
Senior Fellow  
Hoover Institute and Freeman Spogli Institute  
Stanford University

David L. Dill  
Donald E. Knuth Professor, Emeritus, in the School of Engineering and Professor of Computer Science, Stanford University  
Founder of VerifiedVoting.org

Dr. Michael Fischer  
Professor of Computer Science  
Yale University

Adam Ghetti  
Founder / CTO  
Ionic Security Inc.

Susan Greenhalgh  
Policy Director  
National Election Defense Coalition

Dr. Candice Hoke  
Founding Co-Director, Center for Cybersecurity & Privacy Protection  
C|M Law, Cleveland State University

Harri Hursti  
Security Researcher  
Nordic Innovation Labs

Dr. David Jefferson  
Lawrence Livermore National Laboratory

Dr. Douglas W. Jones  
Department of Computer Science  
University of Iowa

Dr. Justin Moore  
Software Engineer  
Google

Dr. Peter G. Neumann  
Chief Scientist  
SRI International Computer Science Lab  
Moderator of the ACM Risks Forum

Dr. Ronald L. Rivest  
Institute Professor  
MIT

Dr. Aviel D. Rubin  
Professor of Computer Science  
Johns Hopkins University
Dr. John E. Savage  
An Wang Professor Emeritus of Computer Science  
Brown University

Dr. Barbara Simons  
IBM Research (Retired)  
Former President, Association for Computing Machinery

Dr. Eugene H. Spafford  
Professor  
Purdue University

Dr. Philip Stark  
Associate Dean, Division of Mathematics and Physical Sciences,  
University of California, Berkeley

Affiliations are for identification purposes only. They do not imply institutional endorsements.
What Voters are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters’ Memories of their Ballots*

Richard A. DeMillo and Robert S. Kadel

Georgia Institute of Technology

and

Marilyn R. Marks

Coalition for Good Governance

November 23, 2018
Revised April 11, 2019

* This research was supported in part by the Coalition for Good Governance
ABSTRACT

As a new generation of voting system technology is deployed in response to concerns about the security of American election infrastructure, the role of voter verification of paper audit trails (VVPAT) has re-emerged as central to ensuring election integrity. A critical step in many electronic voting systems relies on the ability of a voter to carry out what seems at first blush like a simple task: review a computer-generated record of ballot choices made moments before to verify that those choices have been fully and accurately recorded. Prior studies have not addressed what appears to us to be the fundamental question to be resolved if VVPAT is to be a cornerstone of voting technology: can electors verify their votes by reviewing a paper ballot summary? If so, then the paper records are relatively secure evidence of voter intent that can be used to conduct audits and recounts. If not, then adversaries who can compromise voting systems can change votes with impunity. The experiments described in this paper, conducted in 2018 during the May 1 and August 2 Tennessee primary elections, suggest that the answer may be “No.”

In asking this question, we are not concerned so much about the practical problems associated with VVPAT as whether there are fundamental cognitive limitations on the act of verification itself. We present preliminary evidence suggesting that, in actual polling place settings, most voters will not attempt to verify paper ballot summary cards, even when directed to do so. Furthermore, polling place exit interviews of voters who attempt to review their ballots reveal that a statistically significant fraction is unable to recall important details of ballots cast only moments before. Voters either fail to recognize errors in ballots presented to them for verification or fail to recognize that the ballots presented for verification were not the ones they cast. These results are broadly consistent with other recent studies that cast doubt on the
reliability and accuracy of memory recall and are evidence of voter memory errors that would make a verified ballot summary card impossible to rely upon as a reliable source record for a post-election audit.

This study differs from prior studies on VVPATs used with DRE (“Direct Recording Electronic”) machines, as this study is limited to more recent electronic ballot marking device (“BMD”) technology. Such technology involves a voter making choices on a touchscreen machine that produces a ballot summary card (not the full ballot contents). The ballot summary card is inserted into a separate mark sense scanner to complete the vote casting process. A consequence of the results presented here is that voters who cast ballots on compromised ballot marking devices that change votes but who have not securely registered their ballot choices by, for example, hand-marking paper ballots, are generally unable to detect vote manipulation. The implications for future voting system design are also discussed.

INTRODUCTION

The passage of the Help America Vote Act (HAVA)\(^1\) in 2002 and the nearly 4 billion dollars in HAVA funds subsequently disbursed to the states\(^2\) helped usher in the present era of electronic voting based on computer touchscreens. The authors of HAVA anticipated that voter confidence would be a significant factor in widespread acceptance of computerized voting, and they included a requirement for enabling voter verification of ballot choices before votes are electronically tabulated. Although HAVA requires a voter-verified \emph{paper} audit trail (VVPAT)\(^3\), not all voting machines purchased in the years following the law’s enactment printed paper audit trails.\(^4\)\(^5\)\(^6\)
Voting system vendors and a small but influential group of voting technology enthusiasts argued instead that voters could verify their choices on the touchscreens before submitting their ballots.\(^7\) That approach, however, violates the cybersecurity redundancy principle responsible for detecting manipulation\(^8\). Touchscreen displays and electronic records of cast ballots share common modes of failure since they rely on the same memory and computer logic that would be compromised in a successful attack. This lack of independence invalidates any post-election audit that seeks to compare voted ballots with reported election results. To help resolve the question of whether paper is an essential aspect of voter verification, the Auditability Working Group of the Election Assistance Commission (EAC), which HAVA established to oversee implementation, commissioned a study by the National Institute of Standards and Technology (NIST). The resulting 2011 Report\(^9\) to the EAC was unequivocal in finding that paper records for the recording of votes are necessary: “[We] found no alternative that does not have as a likely consequence either an effective requirement for paper records or the possibility of undetectable errors in the recording of votes.”

Paper—hand-marked by a voter in the form of a ballot—is the medium preferred by most experts for recording voter intent, despite a nearly twenty-year campaign by the voting system industry to promote an all-electronic pathway from capturing a digital record of voter intent to tallying and reporting elections results\(^10\). A 2018 report by the National Academy of Sciences\(^11\) summarizes the rationale:

A paper ballot–based voting system makes the paper ballot the official “ballot of record” of the voter’s expressed intentions. Other representations (e.g., an electronic representation produced by a scanner) are derivative and are not voter verifiable.\(^12\)
Nevertheless, many election systems do not regard the ballot marked by the voter as the cast ballot. Some states even rely exclusively on paperless touchscreen systems. In these states, there are no voter-marked ballots. However, many other states have converted to new voting machines that use paper ballots, and those that have not will likely do so when they replace their existing systems. Promoted heavily by the voting machine industry, systems that automatically mark ballots in response to touches on a screen are becoming more common. In such systems, software senses screen touches, records them in computer memory, and subsequently prints them as 1D or 2D barcodes on a human-readable paper card (a “ballot summary card”) for voter verification. Once verified, an electronically produced paper ballot barcode is scanned by a mark sensing device, thereby casting a vote. If a voter verifies the human-readable portion of the ballot summary card, the cast ballot is suitable for use as a VVPAT for of audits and recounts.

Voter verifiability has always been controversial. A working paper from the MIT/Caltech Voting Project focused on security and usability concerns of touchscreen voting units. This study and related research—whether through experiments, election observations, or the design of auditing protocols that require VVPAT—have left unresolved what seems to us the central problem of VVPAT: “…establish that people can verify their ballots using a paper receipt.” In other words, is the very concept of voter verification of electronically created paper trails meaningful?

ELECTRONIC BALLOT MARKING DEVICES

There is no standard definition of what constitutes a verified ballot. Sometimes, ballot summary cards are the official audit records, but summaries may be difficult for voters to verify because of their length or complexity. It is possible that a clever designer might break voter
verification into several smaller steps, which would make summaries easier to verify. This paper avoids such speculation by dealing only with voters’ recollection of their ballots. Our reasoning is as follows: if voters cannot distinguish between correct and incorrect versions of their own ballots, then verifying summaries or other renderings of those ballots is no less error prone since any such verification necessarily includes recall of prior choices as a prerequisite step.

We limit our study to electronic ballot marking devices (BMD)\textsuperscript{18} that use touchscreens to record and print voter choices on paper ballot summary cards. A ballot summary card contains a human-readable summary of the selections made by the voter but not other unselected choices that may have appeared on the ballot. The card may also contain computer-generated marks such as barcodes that encode the official vote and other information that is not in human readable form (see Figure 1). Voters verify these computer-marked summaries and feed them into mark-sense scanners for subsequent tabulation and reporting. Without loss of generality, we assume that the scanners can either sense human readable voter selections or non-human readable encodings of those selections. BMD advocates believe that the act of printing a computer marked ballot summary card and presenting it to the voter for verification before casting the ballot eliminates the need for a hand-marked paper ballot since only a few seconds elapse between the act of voting on the touchscreen and a voter’s examination of the printed ballot summary card. Surely, they assert, a voter will be able to recognize and verify that the printed ballot summary of selections is a correct rendering of the intended votes.

This paper describes the results of experiments aimed at determining the extent to which voters recall ballot choices in realistic voting environments and whether such computer generated ballots are appropriate source documents for post-election audits and recounts. The results reinforce prior studies showing that voters are disinclined to review paper trails for
However, the present paper goes further, demonstrating that, to a statistically significant degree, under conditions favorable to recall, even when attempting to verify ballots, voters cannot accurately recall all prior choices and full ballot contents, even if those choices were made only moments before. We do not, in this paper, propose a mechanism responsible for these limitations, although one plausible explanation is that cognitive limitations associated with short term recall and memory errors play a role. The paper concludes with a discussion of the impact these results should have on the design of future voting systems, particularly those BMD systems that print ballot summaries and non-human readable marks, such as bar codes.

STUDY DESIGN

Study 1: Do voters review their ballot summary cards?

Coalition for Good Governance (CGG) volunteers visited two precincts near Gatlinburg, Tennessee (Sevier County) on May 1, 2018, during the county primary election. The county had recently switched to ES&S ExpressVote ballot marking devices that use touch screens for voting and produce ballot summary cards containing scannable barcode votes and information-only human-readable text of the selections (only) on a ballot summary card. A separate optical scanner reads and records the bar coded votes.

The volunteers were asked to observe voting on the touchscreens machines and record the number of seconds each voter spent reviewing the ballot summary card while standing at the voting machine, en route to the scanner, or while standing at the scanner. Volunteers used the stopwatch on their smartphones to measure the number of seconds. The authors recognize that there can be some variability in how the volunteers observed and counted the number of seconds.
voters spent reviewing their ballot summary cards. We did not establish inter-rater reliability, and, for this reason, we regard the results provided below as preliminary.

**Study 2: Can voters verify their ballot summary cards?**

Before Tennessee’s 2018 primary election, two sample ballots were printed for each party, the first showing the correct races and candidates and the second showing certain errors (see Appendix). On the Republican sample ballot for the precinct being observed, the Tennessee House of Representatives 30th District was replaced with the 29th District. County Commission District 8 was replaced with County Commission District 9, and School Board District 8 was replaced with School Board District 9. On the Democratic sample ballot, the Tennessee House of Representatives 30th District Democratic candidate was replaced with the Republican candidates from the same district. County Commission District 8 was replaced with County Commission District 9, and School Board District 8 was replaced with School Board District 9.

On Tennessee’s primary election day, August 2, 2018, CGG volunteers visited two polling locations outside of Chattanooga for which the sample ballots were created. The volunteers stood outside a 150 feet radius of the polling location, and as voters left, the volunteers engaged voters to ask if they would be willing to respond to a few questions. If the voter responded with a ‘yes,’ the volunteer first asked in which primary they had just voted, Republican or Democratic. The volunteer then chose, at random, either the ballot marked with a red 1 or the ballot marked with a red 2. Volunteers were not told in advance which ballot was correct. The respondent’s party and the number of the ballot were recorded on a data sheet. The voter/respondent was permitted time to review the ballot, then the volunteer asked the respondent, “Is this the ballot you just voted on?” If the respondent answered in the affirmative, they were thanked, and the survey was terminated. If the respondent answered in the negative,
they were asked to describe the errors they saw. Upon recording the voter’s description, the volunteer thanked the voter, and the survey was terminated.

**Study 1 Results**

Bearing in mind the limits to the first study of whether voters reviewed their ballot summary cards before inserting them in the scanner, we solicited observations of voter behavior from CCG staff assigned to two polling locations in Sevier County:

- Eighty-seven voters were observed in Sevier County; 46 at one location and 41 in a second location.
- Forty-six voters were observed reviewing their ballot summary cards (52.9%), while 41 did not review their ballot cards (47.1%). Of the 46 who reviewed their ballot cards, 18 were at the first location visited by the volunteers and 28 at the second location.
- The average time spent by the 46 voters who reviewed their ballot cards was 3.9 seconds (with a standard deviation of 3.8 seconds). The minimum time spent reviewing was one second, and the maximum was 19 seconds. The ballots each contained 18 contests, and it seems unlikely that a quarter-second per contest allowed sufficient time to conduct an effective review.

**Study 2 Results**

One-hundred three respondents were surveyed. Tables 1 through 3 provide the frequencies (counts) of respondents’ party primary, the ballot reviewed, and whether the ballot viewed was the one the respondent had just voted. As shown in Table 1, 68.0% of respondents stated they voted in the Republican primary, and 32.0% stated that they voted in the Democratic primary. Table 2 shows that 60.2% of the sample ballots reviewed were the correct ballot and 39.8% were the incorrect ballot. Out of the 103 respondents, 74.5% stated that the ballot they
reviewed as the correct ballot, and 25.5% stated that the ballot they reviewed was the incorrect ballot. (Five out of the 103 respondents gave no definitive answer to the question.)

As shown in Table 4, of the 98 respondents who gave definitive answers as to the correctness of the ballot, 59 were shown the correct ballot. Of them, 51 (86.4%) correctly identified the correct ballot while eight (13.6%) misidentified the correct ballot as incorrect (a false negative). Thirty-nine respondents were shown the incorrect ballot, and 17 (43.6%) correctly identified that their ballot was incorrect. Twenty-two (56.4%) incorrectly identified the incorrect ballot as correct (a false positive). A chi-square test indicated that these differences are statistically significant.

Those who identified the incorrect ballot gave the following information when asked what errors they saw on the ballot:

- [Candidate name] 3rd or 4th column
- [Candidate name] missing, [candidate name], School Board
- [Candidate name] was on Dem ballot
- [Candidate name] wrong, [other candidate name]
- [listed three candidates’ names], School Board
- [listed three candidates’ names]
- 3 or 4, Dist 9
- 30th rather than 29th and one other
- All but [candidate name]
- Don't recognize [candidate name] or the clerks
- House 30th. Most were unchanged
- Just general. I didn't study it
- Missing [candidate name]
- Mostly the same
- Not Registrar of Deeds, School Board
- Republican candidate listed, [candidate name]
- School board
- School Board off
- School Board, [candidate name] District 9
- Some names are Republican and I want to say School Board is incorrect

Discussion
If voters’ memory of their ballots was accurate and their recognition of the sample ballots was correct, 39.8% should have identified that they were viewing the incorrect ballot. Rather, only 25.5% of respondents stated that their ballot was incorrect. Furthermore, 13.6% of respondents mistakenly reported that the correct ballot was incorrect. Such data indicates either that voters’ memories of the ballots they voted on were incorrect, or that their recognition of the ballot they were viewing was erroneous. In either case, the high number (more than 55%) of false positives, if observed in actual verifications, indicates that most voters would verify compromised ballot summary cards that misstated the votes cast a few seconds before.

IMPLEMENTATIONS FOR ELECTION SYSTEM AUDITABILITY DESIGN

Because voting technology can be used to create competing evidence of voter intent, system designers often search for a “gold standard” ballot that can be retained, protected, and analyzed to determine, for example, whether an error or malicious intrusion has corrupted data used to obtain voting results. The principal reason for preferring paper for ballots of record is the difficulty of systematic, malicious attack on a stack of paper, and the creation of a permanent audit trail for verification of results. This advantage of paper ballots is surprisingly controversial, however. One former Georgia Secretary of State has recently testified as to the contrary in Federal Court. Although it seems evident to us that hand-marked paper ballots are the simplest and most reliable way to determine voter intent, others argue that the sordid history of suspect paper-ballot elections justifies the consideration of more technologically complex solutions.

These are issues that go well beyond the scope of this paper, but our results are not unrelated. Currently marketed and approved voting technologies require some form of “verifiability” by the voter. If voters are asked to recall prior choices (rather than, say, present...
evidence of those choices in the form of a hand-marked ballot), it is legitimate also to ask whether voters with ordinary cognitive skills can reliably do so and whether voters are likely to attempt to verify their ballots.

The act of marking and presenting a hand-marked paper ballot is a direct expression of voter intent. In the authors’ view, no further verification is needed because the self-authenticating paper ballot is an observable signal made by the voter, unfiltered by any intermediate technological filter. Although the voter could have incorrectly signaled a choice, human error is a possible outcome of any methods of voting; such a mistake is attributable to the voter and not to the interference of any third party. The hand-marked ballot is the best evidence of voter intent. Voter verification of an electronically produced paper record is a confirmation of voter intent. It is a kind of test. However, intent is a psychological state and therefore cannot be directly accessed by any verifier. Verification of a ballot summary card involves both willingness to focus on the card after voting, and memory of intent or prior actions. Anyone trying to infer voter intent by asking the voter to verify prior choices runs into two psychological limitations.

The first limitation is that short-term human memory is a scarce cognitive resource. Human beings cannot recall more than a dozen recent information chunks of information\(^{25}\)—certainly not the dozens of choices in densely populated counties and precincts, or even the 18 separate contests in Sevier County, Tennessee.

The second limitation is that cognitive biases intrude on a voter’s accurate recall of prior choices. Existing methods for voter verification amount to “Here, look at this!” There is no reason to believe that this or any verification protocol would be resilient to availability heuristics or the dozens of possible memory errors caused by priming, misattribution, suggestibility, serial positioning, telescoping, or other effects.\(^{26}\) Given the extent to which test subjects are known to
insist on the veracity of recollections that are demonstrably false or to agree with an authoritative-sounding description of events that never happened, the use of recall in VVPAT deserves further evaluation.

In a headlong rush to develop new voting technologies, designers may be sidestepping critical questions whose answers affect the safety of election systems. Reducing the readability of ballot summary cards does not increase one’s ability to verify. Ballot summary verification is likely to be error-prone, and many popular ballot marking devices compound this problem by attaching marks and codes that are not readable with reasonable effort by ordinary voters. The result is a source document that is not a reliable document for post-election audits.
Figure 1. Sample output of ES&S ExpressVote Ballot Marking Device
Tables

Table 1: Primary that respondent voted in

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Democrat</td>
<td>33</td>
<td>32.0</td>
<td>32.0</td>
<td>32.0</td>
</tr>
<tr>
<td>Republican</td>
<td>70</td>
<td>68.0</td>
<td>68.0</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>103</td>
<td>100.0</td>
<td></td>
<td>100.0</td>
</tr>
</tbody>
</table>

Table 2: Ballot reviewed

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid 1 (correct ballot)</td>
<td>62</td>
<td>60.2</td>
<td>60.2</td>
<td>60.2</td>
</tr>
<tr>
<td>2 (incorrect ballot)</td>
<td>41</td>
<td>39.8</td>
<td>39.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>103</td>
<td>100.0</td>
<td></td>
<td>100.0</td>
</tr>
</tbody>
</table>

Table 3: Is this the ballot you just voted on?

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>Cumulative Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid No</td>
<td>25</td>
<td>24.3</td>
<td>25.5</td>
<td>25.5</td>
</tr>
<tr>
<td>Yes</td>
<td>73</td>
<td>70.9</td>
<td>74.5</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>98</td>
<td>95.1</td>
<td></td>
<td>100.0</td>
</tr>
<tr>
<td>Missing</td>
<td>5</td>
<td>4.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>103</td>
<td>100.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Table 4: Is this the ballot you just voted on? * Ballot reviewed Crosstabulation**

<table>
<thead>
<tr>
<th>Is this the ballot you just voted on?</th>
<th>No</th>
<th>Count</th>
<th>1 (correct ballot)</th>
<th>2 (incorrect ballot)</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% within Ballot reviewed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13.6%</td>
<td>43.6%</td>
<td>25.5%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Count</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% within Ballot reviewed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>86.4%</td>
<td>56.4%</td>
<td>74.5%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Count</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% within Ballot reviewed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>100.0%</td>
<td>100.0%</td>
<td>100.0%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chi-sq. = 11.143, signif. $p \leq 0.001$
Appendix: Sample Ballots

Correct Republican Sample Ballot

![Sample Ballot Image]

Electronic copy available at: https://ssrn.com/abstract=3292208
Incorrect Republican Sample Ballot
Key to Incorrect Republican Sample Ballot
Correct Democratic Sample Ballot

<table>
<thead>
<tr>
<th>Governor</th>
<th>State Executive Committeewoman, 10th Senatorial District Vote for One (1)</th>
<th>County Trustee Vote for One (1)</th>
<th>Register of Deeds Vote for One (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Karl Dean</td>
<td>Kyle E. Hedrick (Republican Party Nominee)</td>
<td>Mark K. Hulander (Republican Party Nominee)</td>
<td>Marc Gravitt (Republican Party Nominee)</td>
</tr>
<tr>
<td>Craig Fitzhugh</td>
<td>Write-in</td>
<td>Vote for One (1)</td>
<td>焦点：</td>
</tr>
<tr>
<td>Mezanne Vale Payne</td>
<td>Write-in</td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United States Senate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vote for One (1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phil Bredesen</td>
<td>Kyle E. Hedrick (Republican Party Nominee)</td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
<tr>
<td>Gary Davis</td>
<td>Write-in</td>
<td></td>
<td></td>
</tr>
<tr>
<td>John Wolfe</td>
<td></td>
<td>Write-in</td>
<td></td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United States House of</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Representatives, 3rd Congressional District</td>
<td>vote for one (1)</td>
<td>Write-in</td>
<td></td>
</tr>
<tr>
<td>Vote for One (1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Danielle Mitchell</td>
<td>Jim Coppageyes (Republican Party Nominee)</td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tennessee Senate, 11th Senatorial District Vote for One (1)</td>
<td>Write-in</td>
<td>Larry L. Henry (Republican Party Nominee)</td>
<td>Write-in</td>
</tr>
<tr>
<td>Randall “Randy” Price</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tennessee House of Representatives, 30th Representative District</td>
<td>vote for one (1)</td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
<tr>
<td>Vote for One (1)</td>
<td></td>
<td>Larry L. Henry (Republican Party Nominee)</td>
<td>Write-in</td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td>Tim Boyd (Republican Party Nominee)</td>
<td>Write-in</td>
</tr>
<tr>
<td>Joda Thongphoowa</td>
<td></td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
<tr>
<td>State Executive Committeewoman, 10th Senatorial District Vote for One (1)</td>
<td>Write-in</td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
<tr>
<td>Chris Anderson</td>
<td></td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
<tr>
<td>Write-in</td>
<td></td>
<td>Write-in</td>
<td>Write-in</td>
</tr>
</tbody>
</table>

TO VOTE: You must darken the oval (to the RIGHT of your choice(s)) completely. Each contest will indicate how many ovals you may mark.

To cast a WRITE-IN VOTE: You must darken the oval completely AND WRITE THE NAME of your choice in the space provided.

STATE DEMOCRATIC PARTY & HAMILTON COUNTY GENERAL ELECTION
Incorrect Democratic Sample Ballot
Key to Incorrect Democratic Sample Ballot

<table>
<thead>
<tr>
<th>Office</th>
<th>Candidate Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governor</td>
<td>Karl Dean</td>
</tr>
<tr>
<td>债券错误!gov</td>
<td></td>
</tr>
<tr>
<td>State Executive Committeewoman, 10th Senatorial District</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>债券错误!gov</td>
<td></td>
</tr>
<tr>
<td>United States Senate</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>债券错误!gov</td>
<td></td>
</tr>
<tr>
<td>United States House of</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>Representatives, 3rd</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>Congressional District</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>债券错误!gov</td>
<td></td>
</tr>
<tr>
<td>Tennessee Senate, 11th</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>Senatorial District</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>债券错误!gov</td>
<td></td>
</tr>
<tr>
<td>Tennessee House of</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>Representatives, 30th</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>Representative District</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>债券错误!gov</td>
<td></td>
</tr>
<tr>
<td>State Executive</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>Committeewoman, 10th Senatorial</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>District</td>
<td>Vote for One (1)</td>
</tr>
<tr>
<td>债券错误!gov</td>
<td></td>
</tr>
</tbody>
</table>
3. **52 U.S.C. §§ 20901–21145**: (i) The voting system shall produce a permanent paper record with a manual audit capacity for such system. (ii) The voting system shall provide the voter with an opportunity to change the ballot or correct any error before the permanent paper record is produced. (iii) The paper record produced under subparagraph (A) shall be available as an official record for any recount conducted with respect to any election in which the system is used.
4. https://www.eac.gov/assets/1/1/EAC%20Advisory%202005-004%20How%20to%20determine%20if%20a%20voting%20system%20is%20compliant%20with%20Section%20301(a).pdf

12. Ibid, p. 43
14. The security of such systems depends, among other things, on an assumption that the computer does not also print codes or marks that are not human readable. In some current systems mark sense scanning of ballot receipts is the principle input to downstream software that tallies and reports vote totals. In such cases any non-readable portion of the receipt is a non-observable communication channel that attackers can exploit. This is often the case with systems that scan bar codes (discussed below).
16. vote.caltech.edu
17. ibid
19. cf. 16
22. See Ref. 5
23. Curling v. Kemp transcript (Cox testimony)
25. Miller, G. A. (1956), The magical number seven, plus or minus two: some limits on our capacity for processing information. Psychological Review, **63**(2), 81-97.

DeMillo, Kadel & Marks
April 11, 2019

Electronic copy available at: https://ssrn.com/abstract=3292208
Ballot-marking devices (BMDs) cannot assure the will of the voters

Andrew W. Appel† Richard A. DeMillo†
Princeton University Georgia Tech

Philip B. Stark†
Univ. of California, Berkeley

April 21, 2019

Abstract

Computers, including all modern voting systems, can be hacked and misprogrammed. The scale and complexity of U.S. elections may require the use of computers to count ballots, but election integrity requires a paper-ballot voting system in which, regardless of how they are initially counted, ballots can be recounted by hand to check whether election outcomes have been altered by buggy or hacked software. Furthermore, secure voting systems must be able to recover from any errors that might have occurred.

However, paper ballots provide no assurance unless they accurately record the vote as the voter expresses it. Voters can express their intent by hand-marking a ballot with a pen, or using a computer called a ballot-marking device (BMD), which generally has a touchscreen and assistive interfaces. Voters can make mistakes in expressing their intent in either technology, but only the BMD is also subject to systematic error from computer hacking or bugs in the process of recording the vote on paper, after the voter has expressed it. A hacked BMD can print a vote on the paper ballot that differs from what the voter expressed, or can omit a vote that the voter expressed.

It is not easy to check whether BMD output accurately reflects how one voted in every contest. Research shows that most voters do not review paper ballots.
printed by BMDs, even when clearly instructed to check for errors. Furthermore, most voters who do review their ballots do not check carefully enough to notice errors that would change how their votes were counted. Finally, voters who detect BMD errors before casting their ballots, can correct only their own ballots, not systematic errors, bugs, or hacking. There is no action that a voter can take to demonstrate to election officials that a BMD altered their expressed votes, and thus no way voters can help deter, detect, contain, and correct computer hacking in elections. That is, not only is it inappropriate to rely on voters to check whether BMDs alter expressed votes, it doesn’t work.

Risk-limiting audits of a trustworthy paper trail can check whether errors in tabulating the votes as recorded altered election outcomes, but there is no way to check whether errors in how BMDs record expressed votes altered election outcomes. The outcomes of elections conducted on current BMDs therefore cannot be confirmed by audits. This paper identifies two properties of voting systems, contestability and defensibility, that are necessary conditions for any audit to confirm election outcomes. No commercially available EAC-certified BMD is contestable or defensible.

To reduce the risk that computers undetectably alter election results by printing erroneous votes on the official paper audit trail, the use of BMDs should be limited to voters who require assistive technology to vote independently.

Elections for public office and on public questions in the United States or any democracy must produce outcomes based on the votes that voters express when they indicate their choices on a paper ballot or on a machine. Computers have become indispensable to conducting elections, but computers are vulnerable. They can be hacked—compromised by insiders or external adversaries who can replace their software with fraudulent software that deliberately miscounts votes—and they can contain design errors and bugs—hardware or software flaws or configuration errors that result in misrecording or mis-tabulating votes. Therefore there must be some way, independent of any software in any computers, to ensure that reported election outcomes are correct, i.e., consistent with the expressed votes as intended by the voters.

Voting systems should be software independent, meaning that “an undetected change or error in its software cannot cause an undetectable change or error in an election outcome” [23]. Indeed, version 2.0 of the Voluntary Voting System Guidelines (VVSG 2.0) incorporates this principle [7].

Software independence is similar to tamper-evident packaging: if somebody opens the container and disturbs the contents, it will leave a trace.
While software independence is crucial, it is not enough: who can detect errors and what happens when errors are detected are just as important. Even if individual voters in principle could detect changes to their votes on the BMD-generated ballot, unless voters can provide convincing evidence of problems to the public and unless election officials take appropriate remedies when presented with such evidence, software independence alone does not guarantee that outcome-changing problems—accidental or malicious—can be caught, much less corrected.

To be acceptable, a voting system also must be contestable: We say that voting system is contestable if any change or error in its software that results in a change or error in a reported election outcome can generate public evidence that the reported outcome is not trustworthy. Evidence available only to individual voters\(^1\) does not suffice: “trust me” is not evidence. If a voting system is contestable, it is software independent, but the converse is not necessarily true. If a voting system is not contestable, then problems might never see the light of day, much less be corrected.

Voting systems must also be defensible. We say that a voting system is defensible if, when it reports the correct outcome, it can also generate convincing public evidence that the reported outcome is correct. Evidence available only to an election official or voting system vendor does not suffice: in other words, “trust me” is not evidence. If a voting system is not defensible, then it is vulnerable to “crying wolf”: malicious actors could claim that the system malfunctioned when in fact it did not, and election officials will have no way to prove otherwise.

Rivest and Wack \([23]\) also define a voting system to be strongly software independent if it is software independent and moreover, a detected change or error in an election outcome (due to change or error in the software) can be corrected using only the ballots and ballot records of the current election.\(^2\) Strong software independence combines tamper evidence with a kind of resilience: there’s a way to tell whether faulty software caused a problem, and a way to recover from the problem if it did.

The only known practical technology for a contestable, defensible, strongly software independent voting system is hand-marked paper ballots, kept physically secure,

\(^1\)Specifically, if the voter is selected candidate A on the touchscreen of a BMD, but the BMD prints candidate B on the paper ballot, then this A-vs-B evidence is available to the individual voter, but the voter cannot demonstrate this evidence to anyone else, since nobody else saw—nor should have seen—where the voter touched the screen. Thus, the voting system cannot generate public evidence of errors recording expressed votes, even if those errors altered the reported outcome.

\(^2\)The only alternative remedy would be to void the results of the entire election and conduct a new one.
counted by machine, audited manually, and recountable by hand.⁴

Over 40 states now use some form of paper ballot for most voters [14]. Most of the remaining states are taking steps to adopt paper ballots. But not all voting systems that use paper ballots are equally secure. Some are not software independent. Some are software independent but not contestable or defensible. In this report we explain:

- *Hand-marked paper ballot* systems are the only practical technology for contestable, defensible voting systems.
- *Some ballot-marking devices (BMDs)* can be software independent, but they are neither contestable nor defensible. Hacked or misprogrammed BMDs can alter election outcomes undetectably, and elections conducted using BMDs do not provide public evidence that reported outcomes are correct. Therefore BMDs should not be used by voters who are able to mark an optical-scan ballot with a pen.
- *All-in-one BMD or DRE+VVPAT voting machines* are not software independent, contestable, or defensible. They should not be used in public elections.

**Terminology**

Although a voter may form an intention to vote for a candidate or issue days, minutes, or seconds before actually casting a ballot, that intention is a psychological state that cannot be directly observed by anyone else. Others can have access to that intention through what the voter (privately) expresses to the voting technology by interacting with it, e.g., by making selections on a BMD or marking a ballot by hand.⁴ Voting systems must accurately record the vote as the voter expressed it.

With a *hand-marked paper ballot optical-scan* system, the voter is given a paper ballot on which all choices (candidates) in each contest are listed; next to each candidate

---

³The election must also generate convincing evidence that physical security of the ballots was not compromised, and the audit must generate convincing public evidence that the audit itself was conducted correctly.

⁴We recognize that voters make mistakes in expressing their intentions. For example, they may misunderstand the layout of a ballot or through a perceptual error or lapse of attention make an unintended choice. The use of touchscreen technology does not necessarily correct for such user errors, as every smartphone user who has mistyped an important text message knows. Poorly designed ballots, poorly designed touchscreen interfaces, and poorly designed assistive interfaces increase the rate of error in voters’ expressions of their votes. For the purposes of this report, we assume that properly engineered systems seek to minimize such usability errors.
is a target (typically an oval or other shape) which the voter marks with a pen to indicate a vote. Ballots may be either preprinted or printed (unvoted) at the polling place using ballot on demand printers. In either case, the voter creates a tamper-evident record of intent by marking the printed paper ballot with a pen.

Such hand-marked paper ballots may be scanned and tabulated at the polling place using a precinct-count optical scanner (PCOS), or may be brought to a central place to be scanned and tabulated by a central-count optical scanner (CCOS). Mail-in ballots are typically counted by CCOS machines.

After scanning a ballot, a PCOS machine deposits the ballot in a secure, sealed ballot box for later use in recounts or audits; this is ballot retention. Ballots counted by CCOS are also retained for recounts or audits.\(^5\)

Paper ballots can also be hand counted, but in most jurisdictions (especially where there are many contests on the ballot) this is hard to do quickly; Americans expect election-night reporting of unofficial totals. Hand counting—i.e., manually determining votes directly from the paper ballots—is appropriate for audits and recounts.

A ballot-marking device (BMD) provides a computerized user interface that presents the ballot to voters and captures their expressed selections, for instance, a touchscreen interface or an assistive interface that enables voters with disabilities to vote independently. Voter inputs (expressed votes) are recorded electronically. When a voter indicates that the ballot is complete and ready to be cast, the BMD prints a paper version of the electronically marked ballot. We generally use the term BMD for devices that mark ballots but do not tabulate or retain them, and all-in-one for devices that combine ballot marking, tabulation, and retention into the same paper path.

The paper ballot printed by a BMD may be in the same format as an optical-scan form (e.g., with ovals filled as if by hand) or it may list just the names of the candidate(s) selected in each contest. The BMD may also encode these selections into barcodes or QR codes for optical scanning. We discuss issues with barcodes later in this report.

An all-in-one touchscreen voting machine combines computerized ballot marking, tabulation, and retention in the same paper path. All-in-one machines come in several configurations:

- DRE+VVPAT machines—direct-recording electronic (DRE) voting machines with a voter-verifiable paper audit trail (VVPAT)—provide the voter a touchscreen (or

\(^5\)Regulations and procedures governing custody and physical security of ballots are uneven and in many cases inadequate, but simple to correct because of decades of development of best practices.
other) interface, then print a paper ballot that is displayed to the voter under glass. The voter is expected to review this ballot and approve it, after which the machine deposits it into a ballot box. DRE+VVPAT machines do not contain optical scanners; that is, they do not read what is marked on the paper ballot; instead, they tabulate the vote directly from inputs to the touchscreen or other interface.

- BMD+Scanner all-in-one machines\(^6\) provide the voter a touchscreen (or other) interface to input ballot choices and print a paper ballot that is ejected from a slot for the voter to inspect. The voter then reinserts the ballot into the slot, after which the all-in-one BMD+scanner scans it and deposits it into a ballot box.

**Opscan+BMD with separate paper paths.** At least one model of voting machine (the Dominion ICP320) contains an optical scanner and a BMD in the same cabinet,\(^7\) so that the optical scanner and BMD-printer are not in the same paper path; no possible configuration of the software could cause a BMD-marked ballot to be deposited in the ballot box without human handling of the ballot. We do not classify this as an *all-in-one* machine.

### Hacking

There are many forms of computer hacking. In this analysis of voting machines we focus on the alteration of voting machine software so that it miscounts votes or mismarks ballots to alter election outcomes. There are many ways to alter the software of a voting machine: a person with physical access to the computer can open it and directly access the memory; one can plug in a special USB thumbdrive that exploits bugs and vulnerabilities in the computer’s USB drivers; one can connect to its WiFi port or Bluetooth port or telephone modem (if any) and exploit bugs in those drivers, or in the operating system.

“Air-gapping” a system (which is to say, disconnecting it from a wired network) does not automatically protect it. Before each election, election administrators must transfer a *ballot definition* into the voting machine by inserting a *ballot definition cartridge* that was programmed on election-administration computers that may have been connected previously to various networks; it has been demonstrated that vote-changing viruses can propagate via these ballot-definition cartridges [13].

Hackers might be corrupt insiders with access to a voting-machine warehouse; cor-

---

\(^6\)The ES&S ExpressVote can be configured as either a BMD or a BMD+Scanner all-in-one.

\(^7\)More precisely, the ICP320 optical scanner and the BMD audio+buttons interface are in the same cabinet, but the printer is a separate box.
rupt insiders with access to a county’s election-administration computers; outsiders who can gain remote access to election-administration computers; outsiders who can gain remote access to voting-machine manufacturers’ computers (and “hack” the firmware installed in new machines, or the firmware updates supplied for existing machines), and so on. Supply-chain hacks are also possible: the hardware installed by a voting system vendor may have malware pre-installed by the vendor’s component suppliers.8

Computer systems (including voting machines) have so many layers of software that it is impossible to make them perfectly secure [18, pp. 89–91]. When manufacturers of voting machines use the best known security practices, adversaries may find it more difficult to hack a BMD or optical scanner—but not impossible. Every computer in every critical system is vulnerable to compromise through hacking, insider attacks or exploiting design flaws.

Election assurance through risk-limiting audits.

To ensure that the reported outcome of each contest is that outcome that would have been found by accurately tabulating the voters’ intent as recorded, the most practical known technology is a risk-limiting audit (RLA) of paper ballots [25, 26, 17]. The National Academies of Science, Engineering, and Medicine, recommend routine RLAs after every election [18], as do many other organizations and entities concerned with election integrity.9

A RLA involves manually inspecting randomly selected paper ballots following a rigorous protocol. The audit stops if and when the sample provides convincing evidence that the reported outcome is correct; otherwise, the audit continues until every ballot has been inspected manually and the correct electoral outcome is known.

RLAs can check whether errors in tabulating recorded votes altered election outcomes, but cannot check whether errors in recording expressed votes altered election outcomes. Properly preserved hand-marked paper ballots ensure that expressed votes are identical to recorded votes. On the other hand, BMDs might not record expressed

8Given that many chips and other components are manufactured in China and elsewhere, this is a serious concern. Carsten Schürmann has found Chinese pop songs on the internal memory of voting machines (C. Schürmann, personal communication, 2018). Presumably those files were left there accidentally—but this shows that malicious code could have been pre-installed deliberately, and that neither the vendor’s nor the election official’s security and quality control measures discovered and removed the extraneous files.

9Among them are the Presidential Commission on Election Administration, the American Statistical Association, the League of Women Voters, and Verified Voting Foundation.
votes accurately, for instance, if BMD software has bugs, was misconfigured, or was hacked. Thus, RLAs that rely on BMD output cannot ensure that election outcomes are correct.

RLAs protect against vote-tabulation errors, whether those errors are caused by failures to follow procedures, misconfiguration, miscalibration, faulty engineering, bugs, or malicious hacking. The risk limit of a risk-limiting audit is the maximum chance that an outcome that is incorrect because of tabulation errors will pass the audit without being corrected. The risk limit should be determined as a matter of policy or law. For instance, a 5% risk limit means that, if a reported outcome is wrong because of tabulation errors, there is at least a 95% chance that the post-election audit will correct it. Smaller risk limits give higher confidence in election outcomes, but require inspecting more ballots, other things being equal. RLAs never revise a correct outcome.

RLAs can be very efficient, depending in part on how the voting system is designed. If the computer results are accurate, an efficient RLA with a risk limit of 5% requires examining about (7 divided by the margin) ballots selected randomly from the contest. For instance, if the margin of victory is 10% and the results are correct, the RLA would need to examine about $\frac{7}{10\%} = 70$ ballots to confirm the outcome at 5% risk. For a 1% margin, the RLA would need to examine about $\frac{7}{1\%} = 700$ ballots. The sample size does not depend (much) on the total number of ballot cast in the contest, only on the margin of the winning candidate’s victory.

A paper-based voting system (such as one that uses optical scanners) is systematically more secure than a paperless system (such as DREs) only if the paper trail is trustworthy and the results are audited against the paper trail using a rigorous method such as an RLA.

But what if the paper ballots are not a trustworthy record of the votes expressed by the voters? If it is possible that error, hacking, bugs, or miscalibration caused the recorded votes to differ from the expressed votes, an RLA or even a full hand recount does not provide convincing public evidence that election outcomes are correct: such a system cannot be defendable. In short, paper ballots provide little assurance against hacking if they are never examined or if the paper might not accurately record the vote expressed by the voter.

---

10RLAs do not protect against problems that cause BMDs to print something other than what was shown to the voter on the screen, nor do they protect against problems with ballot custody.

11Technically, it is the diluted margin that enters the calculation. The diluted margin is the number of votes that separate the winner with the fewest votes from the loser with the most votes, divided by the number of ballots cast, including undervotes and invalid votes.
Security Flaws

A BMD-generated paper trail is not a reliable record of the vote expressed by the voter. Like any computer, a BMD (or a DRE+VVPAT) is vulnerable to hacking, installation of unauthorized (fraudulent) software, and alteration of installed software.\textsuperscript{12}

If a hacker sought to steal an election by altering BMD software, what would the hacker program the BMD to do? In cybersecurity practice, we call this the threat model.

The simplest threat model is this one: In some contests, not necessarily top-of-the-ticket, change a small percentage of the votes (such as 5%).

In recent national elections, analysts have considered a candidate who received 60% of the vote to have won by a landslide. Many contests are decided by less than a 10% margin. Changing 5% of the votes can change the margin by 10%, because “flipping” a vote for one candidate into a vote for a different candidate changes the difference in their tallies—i.e., the margin—by 2 votes. If hacking or bugs or misconfiguration could change 5% of the votes, that would be a very significant threat.

Although public and media interest often focus on top-of-the-ticket races such as President and Governor, elections for lower offices such as state representatives, who control legislative agendas and redistricting, and county officials, who manage elections and assess taxes, are just as important in our democracy. But most voters are not as familiar with the names of the candidates for those offices.

Research by one of us \textsuperscript{9}, in a real polling place in Tennessee during the 2018 election, found that half the voters didn’t look at all at the paper ballot printed by a BMD, even when they were holding it in their hand and directed to do so while carrying it from the BMD to the optical scanner. Those voters who did look at the BMD-printed ballot spent an average of 4 seconds examining it to verify that the eighteen or more choices they made were correctly recorded. That amounts to 222 milliseconds per contest, barely enough time for the human eye to move and refocus under perfect conditions and not nearly enough time for perception, comprehension, and recall \textsuperscript{22}.\textsuperscript{13} \textsuperscript{14}

\textsuperscript{12}It is also vulnerable to bugs and misconfiguration.

\textsuperscript{13}You might think, “the voter really should carefully review their BMD-printed ballot.” But because the scientific evidence shows that voters do not \textsuperscript{9} and cognitively cannot \textsuperscript{12} perform this task well, legislators and election administrators should provide a voting system that counts the votes as voters express them.

\textsuperscript{14}Studies of voter confidence about their ability to verify their ballots are not relevant: in typical situations, subjective confidence and objective accuracy are at best weakly correlated. The relationship between confidence and accuracy has been studied in contexts ranging from eyewitness accuracy \textsuperscript{6, 8,}
The same study found that among voters who examined their hand-marked ballots, half were unable to recall key features of ballots cast moments before, a prerequisite step for being able to recall their own ballot choices.

Suppose, then, that 10% of voters examine their paper ballots carefully enough to even see the candidate’s name recorded as their vote for legislator or county commissioner. Of those, perhaps only half will remember the name of the candidate they intended to vote for.\textsuperscript{15}

Of those who notice that the vote printed is not the candidate they intended to vote for, what are they supposed to think, and what are they supposed to do? Do they think, “Oh, I must have made a mistake on the touchscreen,” or do they think, “Hey, the machine is cheating or malfunctioning!” There’s no way for the voter to know for sure—voters do make mistakes—and there’s absolutely no way for the voter to prove to a pollworker or election official that a BMD printed something other than what the voter entered on the screen.\textsuperscript{16}

Either way, polling place procedures generally advise voters to ask a pollworker for a new ballot if theirs does not show what they intended. Pollworkers should void that BMD-printed ballot, and the voter should get another chance to mark a ballot. Anecdotal evidence suggests that many voters are too timid to ask, or don’t know that they have the right to ask, or are not sure whom to ask. Even if a voter asks for a new ballot, training for pollworkers is uneven, and we are aware of no formal procedure for resolving disputes if a request for a new ballot is refused. Moreover, there is no sensible protocol for ensuring that BMDs that misbehave are investigated—nor can there be, as we argue below.

Let’s summarize. If a machine alters votes on 5% of the ballots (enabling it to change the margin by 10%), then optimistically we might expect $\frac{1}{20} \times \frac{1}{10} \times \frac{1}{2}$ or 0.25% of the voters to request a new ballot and correct their vote. This means that the machine will change the margin by 9.75% and get away with it.

In this scenario, 0.25% of the voters, one in every 400 voters, has requested a new ballot. You might think, “that’s a form of detection of the hacking.” But is isn’t, as a

\textsuperscript{28} to confidence in psychological clinical assessments \cite{10} and social predictions \cite{11}. The disconnect is particularly severe at high confidence. Indeed, this is known as “the overconfidence effect.” For a lay discussion, see Thinking, Fast and Slow by Nobel economist Daniel Kahnemann \cite{15}.

\textsuperscript{15} We ask the reader, “do you know the name of the most recent losing candidate for county commissioner?” We recognize that some readers of this document are county commissioners, so we ask those readers to imagine the frame of mind of their constituents.

\textsuperscript{16} Voters should certainly not videorecord themselves voting! That would defeat the privacy of the secret ballot and is illegal in most jurisdictions.
practical matter: a few individual voters may have detected that there was a problem, but there’s no procedure by which this translates into any action that election administrators can take to correct the outcome of the election. Polling place procedures cannot correct or deter hacking, or even reliably detect it, as we discuss next. This is essentially the distinction between a system that is merely software independent and one that is contestable: a change to the software that alters the outcome might generate evidence for an alert, conscientious, individual voter, but it does not generate public evidence that an election official can rely on to conclude there is a problem.

Even if some voters notice that BMDs are altering votes, there’s no way to correct the election outcome. Suppose a state election official wanted to detect whether the BMDs are cheating, and correct election results, based on actions by those few alert voters who notice the error. What procedures could possibly work against the manipulation we are considering?

1. How about, “If at least 1 in 400 voters claims that the machine misrepresented their vote, void the entire election.” No responsible authority would implement such a procedure. A few dishonest voters could collaborate to invalidate entire elections simply by falsely claiming that BMDs changed their votes.

2. How about, “If at least 1 in 400 voters claims that the machine misrepresented their vote, then investigate.” Investigations are fine, but then what? The only way an investigation can ensure that the outcome accurately reflects what voters expressed to the BMDs is to void an election in which the BMDs have altered votes and conduct a new election. But how do you know whether the BMDs have altered votes, except based the claims of the voters? Furthermore, the investigation itself would suffer from the same problem as above: how can one distinguish between voters who detected BMD hacking or bugs from voters who just want to interfere with an election?

This is the essential security flaw of BMDs: few voters will notice and promptly report discrepancies between what they saw on the screen and what is on the BMD print-

17Note that in many jurisdictions, far fewer than 400 voters use a given machine on election day: BMDs are typically expected to serve fewer than 300 voters per day. (The vendor ES&S recommended 27,000 BMDs to serve Georgia’s 7 million voters, amounting to 260 voters per BMD [24].) Recall also that the rate 1 in 400 is tied to the amount of manipulation. What if the malware flipped only one vote in 50, instead of 1 vote in 20? That could still change the margin by 4%, but—in this hypothetical—would be noticed by only one voter in 1,000, rather than one in 400. The smaller the margin, the less manipulation it would have taken to alter the electoral outcome.

18Forensic examination of the BMD might show that it was hacked or misconfigured, but it cannot prove that the BMD was not hacked or misconfigured.
out, and even when they do notice, there’s nothing appropriate that can be done. (Nor should it be the responsibility of voters to test voting-machine security and accuracy—this is a difficult burden that should not be placed on the voters.)

Therefore, BMDs should not be used by most voters.

**Why can’t we rely on pre-election and post-election logic and accuracy testing?** Most, if not all, jurisdictions perform some kind of *logic and accuracy testing* (LAT) of voting equipment before elections. LAT generally involves voting on the equipment using various combinations of selections, then checking whether the equipment tabulated the votes correctly. As the Volkswagen/Audi “Dieselgate” scandal shows, devices can be programmed to behave properly when they are tested but misbehave in use. Therefore, LAT can never prove that voting machines performed properly in practice.

**Don’t voters need to check hand-marked ballots, too?** It is always a good idea to check one’s work. The difference is, with hand-marked paper ballots, voters are responsible for catching and correcting *their own errors*, while if BMDs are used, voters are also responsible for catching *machine errors, bugs, and hacking*. Voters are the only people who can detect such problems with BMDs—but, as explained above, if voters do find problems, there’s no way they can prove to poll workers or election officials that there were problems and no way to ensure that election officials take appropriate remedial action.

**Other tradeoffs, BMDs versus hand-marked opscan**

Supporters of ballot-marking devices advance several other arguments for their use.

- **Mark legibility.** A common argument is that a properly functioning BMD will generate clean, error-free, unambiguous marks, while hand marked paper ballots may contain mistakes and stray marks that make it impossible to discern a voter’s intent. However appealing this argument seems at first blush, the data are not nearly so compelling. Experience with statewide recounts in Minnesota and elsewhere suggest that truly ambiguous handmade marks are very rare.\(^{19}\) For instance, 2.9 million hand-marked ballots were cast in the 2008 Minnesota race.

\(^{19}\)States do need clear and complete regulations for interpreting voter marks.
between Al Franken and Norm Coleman for the U.S. Senate. In a manual recount, between 99.95% and 99.99% of ballots were unambiguously marked.\footnote{During the recount, the Coleman and Franken campaigns initially challenged a total of 6,655 ballot-interpretation decisions made by the human recounters. The State Canvassing Board asked the campaigns to voluntarily withdraw all but their most serious challenges, and in the end approximately 1,325 challenges remained. That is, approximately 5 ballots in 10,000 were ambiguous enough that one side or the other felt like arguing about it. The State Canvassing Board, in the end, classified all but 248 of these ballots as votes for one candidate or another. That is, approximately 1 ballot in 10,000 was ambiguous enough that the bipartisan recount board could not determine an intent to vote.” [1] See also [20].}

In addition, usability studies of hand marked bubble ballots—the kind in most common use in U.S. elections—indicate a voter error rate of 0.6%, much lower than the 2.5–3.7% error rate for machine-marked ballots\footnote{We have found that some local election officials consider marks to be ambiguous if machines cannot read the marks. That is a different issue from humans not being able to interpret the marks. Errors in machine interpretation of voter intent can be dealt with by manual audits: if the reported outcome is wrong because machines misinterpreted handmade marks, a RLA has a known, large chance of correcting the outcome.}.\footnote{Better designed user interfaces (UI) might reduce the error rate for machine-marked ballots below the historical rate for DREs; however, UI improvements cannot keep BMDs from printing something other than what the voter is shown on the screen.} Moreover, modern image-based opscan equipment is better than older “marksense” machines at interpreting imperfect marks. Thus, mark legibility is not a good reason to adopt BMDs for all voters.

- **Undervotes, overvotes.** Another argument offered for BMDs is that the machines can alert voters to undervotes and prevent overvotes. That is true, but modern PCOS can also alert a voter to overvotes and undervotes, allowing a voter to eject the ballot and correct it. Other solutions, such as non-tabulating scanners that simply warn voters of overvotes and undervotes on hand-marked ballots, would be less risky than BMDs.

- **Bad ballot design.** Ill-designed paper ballots, just like ill-designed touchscreen interfaces, may lead to unintentional undervotes\footnote{Electronic copy available at: https://ssrn.com/abstract=3375755} [19]. For instance, the 2006 Sarasota, Florida, touchscreen ballot was badly designed. The 2018 Broward County, Florida, opscan ballot was badly designed: it violated three separate guidelines from the EAC’s 2007 publication, “Effective Designs for the Administration of Federal Elections, Section 3: Optical scan ballots.” [27] In both of these cases (touchscreens in 2006, hand-marked optical-scan in 2018), undervote rates were high. The solution is to follow standard, published ballot-design guidelines and other best practices, both for touchscreens and for hand-marked ballots [3, 19].

- **Low-tech paper-ballot fraud.** All paper ballots, however they are marked, are vulnerable to loss, ballot-box stuffing, alteration, and substitution between the
time they are cast and the time they are recounted. That’s why it is so important to make sure that ballot boxes are always in multiple-person (preferably bipartisan) custody at any time when they are handled, and that appropriate physical security measures are in place. Strong, verifiable chain-of-custody protections are essential.

Hand-marked paper ballots are vulnerable to alteration by anyone with a pen. Both hand-marked and BMD-marked paper ballots are vulnerable to substitution: anyone who has poorly supervised access to a legitimate BMD during election day can create fraudulent ballots, not necessarily to deposit them in the ballot box immediately (in case the ballot box is well supervised on election day) but with the hope of substituting it later in the chain of custody.23

All those attacks (on hand-marked and on BMD-marked paper ballots) are fairly low-tech. There are also higher-tech ways of producing ballots indistinguishable from BMD-marked ballots for substitution into the ballot box, where there is inadequate chain-of-custody protection.

- **Accessible voting technology.** If everyone voted on a BMD, it would guarantee that an accessible device had been set up in the polling place for all voters who needed one. But this is not a good reason to adopt BMDs for all voters. Among other things, it would expose all voters to the security flaws described above, decreasing public confidence in the entire election. Some accessibility advocates argue that requiring disabled voters to use BMDs compromises their privacy since hand marked ballots are easily distinguishable from machine marked ballots. This argument has been undercut by the availability in the marketplace of BMDs that mark ballots that cannot easily be distinguished from hand marked ballots. Other advocates object to the idea that disabled voters must use a different method of marking ballots, arguing that their rights are thereby violated. Both HAVA and ADA require accommodations for voters with physical and cognitive impairments, but neither law requires that those accommodations must be used by all voters. To best enable and facilitate participation by all voters, each voter should be provided with a means of casting a vote best suited to their abilities.

- **Ballot printing costs.** Preprinted optical-scan ballots cost 20–50 cents each.24 Blank cards for BMDs cost up to 15 cents each, depending on the make and model of BMD.25 But optical-scan ballots must be preprinted for as many vot-

---

23Some BMDs print a bar-code indicating when and where the ballot was produced, but that does not prevent such a substitution attack against currently EAC-certified, commercially available BMDs. We understand that systems under development might make ballot-substitution attacks against BMDs more difficult.

24Single-sheet (one- or two-side) ballots cost 20-28 cents, double-sheet ballots needed for elections with many contests, up to 50 cents.

25Ballot cards for ES&S ExpressVote cost about 15 cents. New Hampshire’s (One4All / Prime III)
ers as might show up, whereas blank BMD cards are consumed in proportion to how many voters do show up. The Open Source Election Technology Institute (OSET) conducted an independent study of total life cycle costs\(^\text{26}\) for hand-marked paper ballots and BMDs in conjunction with the 2019 Georgia legislative debate regarding BMDs\(^\text{21}\). OSET concluded that, even in the most optimistic (i.e., lowest cost) scenario for BMDs and the most pessimistic (i.e., highest cost) scenario for hand-marked paper ballots and ballot-on-demand (BOD) printers—which can print unmarked ballots as needed—the total lifecycle costs for BMDs would be higher than the corresponding costs for hand marked paper ballots.\(^\text{27}\)

- **Vote centers.** To run a vote center that serves many election districts with different ballot styles, one must be able to provide each voter a ballot containing the contests that voter is eligible to vote in, possibly in a number of different languages. This is easy with BMDs, which can be programmed with all the appropriate ballot definitions. With preprinted optical-scan ballots, the PCOS can be programmed to accept many different ballot styles, but the vote center must still maintain inventory of many different ballots. BOD printers are another economical alternative for vote centers.\(^\text{28}\)

- **Paper/storage.** BMDs that print summary cards rather than full-face ballots can save paper and storage space. However, many BMDs print full-face ballots, while many BMDs that print summary cards use thermal printers and paper that is fragile and can fade in a few months.\(^\text{29}\)

Advocates of hand-marked paper ballot systems advance these additional arguments.

\(^{26}\) BMDs used by sight-impaired voters use plain paper that is less expensive.

\(^{27}\) They include not only the cost of acquiring and implementing systems but also the ongoing licensing, logistics, and operating (purchasing paper stock, printing, and inventory management) costs.

\(^{28}\) BOD printers currently on the market arguably are best suited for vote centers, but less expensive options suited for polling places could be developed. Indeed, BMDs that print full-face ballots could be re-purposed as BOD printers for polling place use, with modest changes to the programming.

\(^{29}\) Ballot-on-demand printers may require maintenance such as replacement of toner cartridges. This is readily accomplished at a vote center with a professional staff. Ballot-on-demand printers may be a less attractive option for many small precincts on election day, where there is no professional staff—but on the other hand, they are less necessary, since far fewer ballot styles will be needed in any one precinct.

• **Cost.** Using BMDs for all voters substantially increases the cost of acquiring, configuring, and maintaining the voting system. One PCOS can serve 1200 voters in a day, while one BMD can serve only about 260 [24]—though both these numbers vary greatly depending on the length of the ballot and the length of the day. OSET analyzed the relative costs of acquiring BMDs for Georgia’s nearly seven million registered voters versus a system of hand marked paper ballots, scanners, and BOD printers [21]. A BMD solution for Georgia would cost taxpayers between 3 and 5 times the cost of a system based on hand marked paper ballots.

• **Mechanical reliability and capacity.** Pens are likely to have less downtime than BMDs. It is easy and inexpensive to get more pens and privacy screens when additional capacity is needed. If a precinct-count scanner goes down, people can still mark ballots with a pen; if the BMD goes down, voting stops. Thermal printers used in DREs with VVPAT are prone to jams; those in BMDs might have similar flaws.

These secondary pros and cons of BMDs do not outweigh the primary security and accuracy concern: BMDs, if hacked or erroneous, can change votes in a way that is not correctable. BMD voting systems are not contestable, defensible, or strongly software independent. Therefore, ballots cast by BMD cannot effectively be audited.

**Barcodes**

A controversial feature of some BMDs allows them to print 1-dimensional or 2-dimensional barcodes on the paper ballots. A 1-dimensional barcode resembles the pattern of vertical lines used to identify products by their universal product codes. A 2-dimensional barcode or QR code is a rectangular area covered in coded image modules that encode more complex patterns and information. BMDs print barcodes on the same paper ballot that contains human-readable ballot choices. Voters using BMDs are expected to verify the human-readable printing on the paper ballot card, but the presence of barcodes with human-readable text poses some significant problems.

• **Barcodes are not human readable.** The whole purpose of a paper ballot is to be able to recount (or audit) the voters’ votes in a way independent of any (possibly hacked or buggy) computers. If the official vote on the ballot card is the barcode, then it is impossible for the voters to verify that the official vote they cast is the vote they expressed. Therefore, before a state even considers using BMDs that print barcodes (and we do not recommend doing so), the State must ensure by statute that recounts and audits are based only on the human-readable portion of
the paper ballot. Even so, audits based on untrusted paper trails suffer from the verifiability the problems we outlined above.

- **Ballot cards with barcodes contain two different votes.** Suppose a state does ensure by statute that recounts and audits are based on the human-readable portion of the paper ballot. Now a BMD-marked ballot card with both barcodes and human-readable text contains two different votes in each contest: the barcode (used for electronic tabulation), and the human-readable selection printout (official for audits and recounts). In few (if any) states has there even been a discussion of the legal issues raised when the official markings to be counted differ between the original count and a recount.

- **Barcodes pose technical risks.** Any coded input into a computer system—including wired network packets, WiFi, USB thumbdrives, and barcodes—pose the risk that the input-processing software can be vulnerable to attack via deliberately ill-formed input. Over the past two decades, many such vulnerabilities have been documented on each of these channels (including barcode readers) that, in the worst case, give the attacker complete control of a system. If an attacker were able to compromise a BMD, the barcodes are an attack vector for the attacker to take over an optical scanner (PCOS or CCOS), too. Since it is good practice to close down all such unneeded attack vectors into PCOS or CCOS voting machines (e.g., don’t connect your PCOS to the Internet!), it is also good practice to avoid unnecessary attack channels such as barcodes.

### End-to-End Verifiable BMDs

In all BMD systems currently on the market, and in all BMD systems certified by the EAC, the printed ballot or ballot summary is the only channel by which voters can verify the correct recording of their ballots, independently of the computers. The analysis in this paper applies to all of those BMD systems.

There is a class of voting systems called “end-to-end verifiable” (E2E-V), which provide an alternate mechanism for voters to verify their votes [2]. Some E2E-V systems incorporate BMDs, for instance STAR-Vote\(^\text{31}\) [5]. If such a voting system could

---

30 An example of a barcode attack is based on the fact that many commercial barcode-scanner components (which system integrators use to build cash registers or voting machines) treat the barcode scanner using the same operating-system interface as if it were a keyboard device; and then some operating systems allow “keyboard escapes” or “keyboard function keys” to perform unexpected operations.

31 The STAR-Vote system is actually a DRE+VVPAT system with a smart ballot box, rather than a BMD system: voters interact with a device that captures their votes electronically and prints a paper record that voters can inspect, but the electronic votes are held “in limbo” until the paper ballot is de-
be demonstrated to be contestable, defensible, and adequately usable by voters, then
the analysis in this paper might not be applicable to such BMDs. No E2E-V systems
are currently certified by the EAC, nor to our knowledge is any such system under re-
view for certification, nor are any of the 5 major voting-machine vendors offering such
a system for sale.\textsuperscript{32}

\begin{bold}{Design Flaws in All-in-One BMDs}\end{bold}

Some voting machines incorporate a BMD interface, printer, and optical scanner into
the same cabinet. Other DRE+VVPAT voting machines incorporate ballot-marking,
tabulation, and paper-printout retention, but without scanning.

These are often called “all-in-one” voting machines. Any such machine that in-
cludes \textit{ballot marking} and \textit{deposit into the ballot box} in the same paper path, is unsafe.

Using an all-in-one machine, the voter makes choices on a touchscreen or through
a different accessible interface. When the selections are complete, the BMD prints the
completed ballot for the voter to review and verify, before depositing the ballot in a
ballot box attached to the machine.

- The ES&S ExpressVote (in all-in-one mode) allows the voter to mark a ballot by
touchscreen or audio interface, then prints a paper ballot card and ejects it from a
slot. The voter has the opportunity to review the ballot, then the voter redep-
sits the ballot into the same slot, where it is scanned and deposited into a ballot box.

- The ES&S ExpressVoteXL allows the voter to mark a ballot by touchscreen or
audio interface, then prints a paper ballot (cash-register tape format) and displays
it under glass. The voter has the opportunity to review the ballot, then the voter
touches the screen to indicate “OK,” and the machine pulls paper ballot up (still
under glass) and into the integrated ballot box.

- The Dominion ImageCast Evolution (ICE) allows the voter to deposit a hand-
marked paper ballot, which it scans and drops into the attached ballot box. \textit{Or},
a voter can use a touchscreen or audio interface to direct the marking of a paper
ballot, which the voting machine ejects through a slot for review; then the voter

\textsuperscript{32}Some vendors, notably Scytl, have sold systems advertised as E2E-V in other countries. Those sys-
tems were not in fact E2E-V. Moreover, serious security flaws have been found in their implementations.
See, e.g., [16].
redeposits the ballot into the slot, where it is scanned and dropped into the ballot box.

In all three of these machines, the ballot-marking printer is in the same paper path as the mechanism to deposit marked ballots into an attached ballot box. This opens up a very serious security vulnerability: the voting machine can mark the paper ballot (to add votes or spoil already-cast votes) after the last time the voter sees the paper, and then deposit that marked ballot into the ballot box without the possibility of detection.

Vote-stealing software could easily be constructed that looks for undervotes on the ballot, and marks those unvoted spaces for the candidate of the hacker’s choice. This is very straightforward to do on optical-scan bubble ballots (as on the Dominion ICE) where undervotes are indicated by no mark at all. On machines such as the ExpressVote and ExpressVoteXL, the normal software indicates an undervote with the words NO SELECTION MADE on the ballot summary card. Hacked software could simply leave a blank space there (most voters wouldn’t notice the difference), and then fill in that space and add a matching bar code after the voter has clicked “cast this ballot.”

An even worse feature of the ES&S ExpressVote and the Dominion ICE is the auto-cast configuration setting (in the manufacturer’s standard software) that allows the voter to indicate, “don’t eject the ballot for my review, just print it and cast it without me looking at it.” If fraudulent software were installed in the ExpressVote, it could change all the votes of any voter who selected this option, because the voting machine software would know in advance of printing that the voter had waived the opportunity to inspect the printed ballot. We call this auto-cast feature “permission to cheat” [4].

Regarding these all-in-one machines, we conclude:

- Any machine with ballot printing in the same paper path with ballot deposit is not software independent; it is not the case that “an error or fault in the voting system software or hardware cannot cause an undetectable change in election results.” Therefore such all-in-one machines do not comply with the VVSG 2.0 (the Election Assistance Commission’s Voluntary Voting Systems Guidelines).
- All-in-one machines on which all voters use the BMD interface to mark their ballots (such as the ExpressVote and ExpressVoteXL) also suffer from the same serious problem as ordinary BMDs: most voters do not review their ballots effectively, and elections on these machines are not contestable or defensible.
- The auto-cast option for a voter to allow the paper ballot to be cast without human inspection is particularly dangerous, and states must insist that vendors disable or eliminate this mode from the software. However, even disabling the auto-cast feature does not eliminate the risk of undetected vote manipulation.
Remark. The Dominion ImageCast Precinct ICP320 is a precinct-count optical scanner (PCOS) that also contains an audio+buttons ballot-marking interface for disabled voters. This machine can be configured to cast electronic-only ballots from the BMD interface, or an external printer can be attached to print paper optical-scan ballots from the BMD interface. When the external printer is used, that printer’s paper path is not connected to the scanner+ballot-box paper path (a person must take the ballot from the printer and deposit it into the scanner slot). Therefore this machine is as safe to use as any PCOS with a separate external BMD.

Conclusion

Ballot-Marking Devices produce ballots that do not necessarily record the vote expressed by the voter when they enter their selections on the touchscreen: hacking, bugs, and configuration errors can cause the BMDs to print votes that differ from what the voter entered and verified electronically. Furthermore, in cases where the BMD-marked paper ballot does not record the expressed vote, the election system overall is not contestable or defensible, meaning that errors in elections conducted on compromised BMDs cannot be reliably detected or corrected, and that election officials cannot provide convincing evidence that correct reported outcomes of elections conducted using BMDs are indeed correct. Therefore BMDs should not be used by voters who can use hand-marked paper ballots.

All-in-one voting machines, that combine ballot-marking and ballot-box-deposit into the same paper path, are even worse. They have all the disadvantages of BMDs (they are neither contestable or defensible), and they can mark the ballot after the voter has inspected it. Therefore they are not even software independent, and should not be used by those voters who are capable of marking, handling, and visually inspecting a paper ballot.

When computers are used to record votes, the original transaction (the voter’s expression of the votes) is not documented in a verifiable way.\textsuperscript{33} When pen-and-paper is used to record the vote, the original expression of the vote is documented in a verifiable way (provided that secure chain of custody of paper ballots is maintained). Therefore, audits of elections conducted with BMDs cannot ensure that reported outcomes are correct, while audits of elections conducted with hand-marked paper ballots, counted by optical scanners, can.

\textsuperscript{33}It is conceivable that cryptographic protocols used in E2E-V systems could be used to create BMD-based systems that are contestable and defensible, but no such system exists, nor, to our knowledge, has such a design been worked out in principle.
References


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

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

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

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

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

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

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

1. **Mark legibility.** A properly functioning BMD will generate clean, unambiguous marks. However, experience with statewide recounts in Minnesota and elsewhere suggest that truly ambiguous handmade marks are very rare.¹ Thus mark legibility is not a good reason to adopt BMDs for all voters.

2. **Availability of accessible options.** If everyone voted on an accessible device, it would guarantee that an accessible device had been set up for voters who benefit from using one. This is not a good reason to adopt BMDs for all voters.

3. **Paper/storage.** BMDs that print summary cards rather than full-face ballots can save paper and storage space. That would be an advantage for BMDs, but for the security and cost issues. However, evidence suggests that the usability of summary cards to verify one’s selections is very problematic, especially for long ballots with many contests. To my knowledge, there has been no testing of summary ballots or BMD-printed ballots for usability for voter verification.

4. **Cost.** Using BMDs for all voters substantially increases the cost of acquiring, configuring, and maintaining the voting system.

5. **Mechanical reliability and capacity.** Pens are likely to have less downtime than BMDs. It is easy and inexpensive to get more pens and privacy booths. If a precinct-count scanner goes down, people can still mark ballots with a pen; if the BMD goes down, voting stops.

6. **Security and responsibility.** I believe that a well designed and perfectly functioning BMD can help a voter avoid undervotes and other errors *as long as the device is trustworthy*. The problem is that no computer can be trusted to be running the software it is supposed to be running, nor can any software be trusted to be bug-free, especially in a high-stakes “critical infrastructure” role such as

---
¹States do need clear and complete regulations for adjudicating voter intent from voter marks.
recording and tabulating votes. BMDs have all the security and configuration vulnerabilities of the direct-recording electronic (DRE) devices currently used in Georgia. A voter might make his/her selections perfectly on the screen—and verify those selections—but the BMD could print something else on the paper, through error or malfeasance. Only the voter can check for that: auditors can only see what’s on the paper. This is where security falls apart for BMDs. Universal use of BMDs makes every voter responsible for checking whether the BMD is functioning correctly, but a BMD does not give voters the evidence they would need to prove that a machine registered their vote incorrectly.2 This is obviously a bad combination. According to the available evidence,

- very few voters check the BMD printout
- when they do, they generally do not notice errors
- if they notice errors, shame or inconvenience might keep them from requesting another ballot
- if they notice problems, there is no way for a voter to prove that the BMD printed the wrong thing, rather than that the voter erred, so there’s no way to catch a cheating or misconfigured BMD
- pollworkers are not trained to take a machine offline (and start a forensic investigation) if a number of voters complain that the BMD is printing their selections incorrectly.

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

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

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

---

2 Auditors can check whether an opscan system is functioning correctly, but not whether the BMD printed the voter’s selections correctly.
ballots for voters who have the dexterity and vision to use them.

Sincerely,

Philip B. Stark