Evidence-Based Elections, Risk-Limiting Audits, BMDs, QR Codes, and Georgia

Georgia House of Representatives
Blue-Ribbon Study Committee on Election Procedures
Savannah, GA

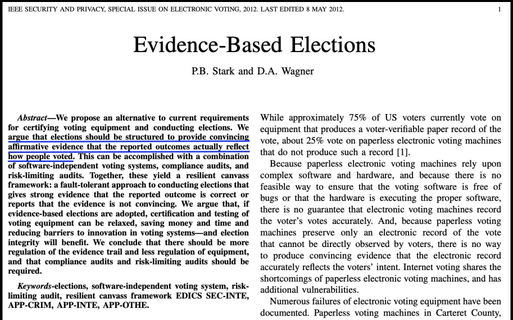
Philip B. Stark

18 September 2025

University of California, Berkeley

- Professor of Statistics at UC Berkeley since 1988
- CA SoS 2007 Post-Election Audit Standards Working Group
- Invented risk-limiting audits (RLAs) 2007; first pilots & publications 2008
- Introduced evidence-based elections 2012
- Helped pilot & implement RLAs and RLA laws in several states starting in 2008
- Wrote first software for RLAs, basis of most or all legit RLA software
- EAC Board of Advisors 2016-2025
- Consulted for SoSs of California, Colorado, New Hampshire
- Expert witness in *Curling v. Raffensperger*
- Helped train election officials in many states

- Not enough to announce winners: should also provide strong *affirmative public* evidence that the reported winners really won.
- "We've never seen a problem" isn't affirmative evidence–especially if you don't look.
- "Our elections are secure" isn't evidence.
- Nor is "trust me."



Evidence-Based Elections

P.B. Stark and D.A. Wagner

***Abstract*—We propose an alternative to current requirements for certifying voting equipment and conducting elections. We argue that elections should be structured to provide convincing affirmative evidence that the reported outcomes actually reflect how people voted. This can be accomplished with a combination of software-independent voting systems, compliance audits, and risk-limiting audits. Together, these yield a resilient canvass framework: a fault-tolerant approach to conducting elections that gives strong evidence that the reported outcome is correct or reports that the evidence is not convincing. We argue that, if evidence-based elections are adopted, certification and testing of voting equipment can be relaxed, saving money and time and reducing barriers to innovation in voting systems—and election integrity will benefit. We conclude that there should be more regulation of the evidence trail and less regulation of equipment, and that compliance audits and risk-limiting audits should be required.**

***Keywords*-elections, software-independent voting system, risk-limiting audit, resilient canvass framework EDICS SEC-INTE, APP-CRIM, APP-INTE, APP-OTHE.**

While approximately 75% of US voters currently vote on equipment that produces a voter-verifiable paper record of the vote, about 25% vote on paperless electronic voting machines that do not produce such a record [1].

Because paperless electronic voting machines rely upon complex software and hardware, and because there is no feasible way to ensure that the voting software is free of bugs or that the hardware is executing the proper software, there is no guarantee that electronic voting machines record the voter's votes accurately. And, because paperless voting machines preserve only an electronic record of the vote that cannot be directly observed by voters, there is no way to produce convincing evidence that the electronic record accurately reflects the voters' intent. Internet voting shares the shortcomings of paperless electronic voting machines, and has additional vulnerabilities.

Numerous failures of electronic voting equipment have been documented. Paperless voting machines in Carteret County,

- RLAs limit *risk that a wrong outcome will be certified*.
- RLAs *require* trustworthy record of the votes.
- If vote record isn't trustworthy, no audit can limit the risk:
    - RLA procedures then distract, not protect
    - this is Georgia today
- If audit lacks legal power to correct wrong outcomes, can't limit risk.
- Auditing some contests doesn't show any other contest was decided correctly.

When Audits and Recounts Distract from Election Integrity: The 2020 U.S. Presidential Election in Georgia

To appear in Proceedings of E-Vote-ID 2024, LNI

Philip B. Stark[1]

Abstract: The U.S. state of Georgia was central to efforts to overturn the results of the 2020 Presidential election, including a phone call from then-president Donald Trump to Georgia Secretary of State Brad Raffensperger asking Raffensperger to 'find' 11,780 votes. Raffensperger has maintained that a '100% full-count risk-limiting audit' and a machine recount agreed with the initial machine-count results, which proved that the reported election results were accurate and that 'no votes were flipped.' While there is no evidence that the reported outcome is wrong, neither is there evidence that it is correct: the two machine counts and the manual 'audit' tallies disagree substantially, even about the number of ballots cast. Some ballots in Fulton County, Georgia, were included in the original count at least twice; some were included in the machine recount at least thrice. Audit handcount results for some tally batches were omitted from the reported audit totals; reported audit results do not include all the votes the auditors counted. In short, the two machine counts and the audit were not probative of who won because of poor processes and controls: a lack of secure physical chain of custody, ballot accounting, pollbook reconciliation, and accounting for other election materials such as memory cards. Moreover, most voters used demonstrably untrustworthy ballot-marking devices; as a result, even a perfect handcount or audit would not necessarily reveal who really won. True risk-limiting audits (RLAs) and rigorous recounts can limit the risk that an incorrect electoral outcome will be certified rather than being corrected. But no procedure can limit that risk without a trustworthy record of the vote. And even a properly conducted RLA of some contests in an election does not show that any other contests in that election were decided correctly. The 2020 U.S. Presidential election in Georgia illustrates unrecoverable errors that can render recounts and audits 'security theater' that distract from the more serious problems rather than justifying trust.

Keywords: risk-limiting audit, election recount, evidence-based elections

To have evidence-based elections or to limit the risk of certifying wrong outcomes, need to create trustworthy record, then keep it trustworthy and audit rigorously.

- BMDs are pens that can be hacked or misconfigured: printout isn't trustworthy
- Images are not trustworthy
- HMPB *starts* trustworthy–but have to keep records safe & organized
  - GA lacks physical ballot accounting, pollbook reconciliation & other sanity checks
  - GA lacks meaningful canvass
- GA's so-called "RLAs" don't limit the risk of certifying wrong outcomes

- Equipment storage not consistently locked or surveilled
- "Sleepovers" in churches, rec centers, etc. where many have access
- Insider access, insiders giving outsiders access
- Testimony that BMDs are not sealed daily during early voting
- Seals easily defeated
- Inadequate seal protocols
- SoS tells jurisdictions to ignore/replace broken or missing seals

Michael Barnes, Director of Center for Election Systems, GA SoS

Message

From: Barnes, Michael [/O=SOS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=D4F658ED134C4A6D91A27F28A0572934-BARNES, MICHAEL]
Sent: 7/9/2020 5:54:46 PM
To: clinchelections@clinchcountyga.gov
Subject: Re: Data Seals

No, just please put your own seal on the equipment and document the seal number attached.

Sent from my iPhone
Michael Barnes
470-316-2884

On Jul 9, 2020, at 1:52 PM, "clinchelections@clinchcountyga.gov" <clinchelections@clinchcountyga.gov> wrote:

EXTERNAL EMAIL: Do not click any links or open any attachments unless you trust the sender and know the content is safe.

<image001.gif>

Michael,
My tech is doing L&A testing and discovered that 2 of our BMDs Election Data Seals were missing, (poll workers). Do we need to send these back to be resealed ? If so my regional tech has offered to take them back to Atlanta and drop them off on his way back home. Please let me know what we need to do.

Laina Ballance
Clinch County Elections Supervisor
25 Court Sq. Suite A
Homerville Ga. 31634
912-487-3656 Office
912-487-5162 Fax
clinchelections@clinchcountyga.gov

State Training Is Grossly Inadequate For Election Security

From: Watson, Frances <fw
Sent: Thursday, November
To: Germany, Ryan <germa
Subject:

Name: Laura Jones
Phone: [redacted]
Address: [redacted]
City: Atlanta
State: GA
Zip Code: [redacted]
County: Fulton
E-mail: [redacted]

Location of Violation: Temp

Confidential

Description of Violation: When we opened the large cabinets containing the voting machines, we discovered that most of the voting machines "election database" doors were wide open and not secured with a zip tie with serial number. Seals were already broken or a zip tie was put on but was not put through the door. Also, we found two paper ballots on the printer. We did not scan these ballots. Our Poll Manager, Kaira Bell, put these on her clipboard. I don't know where those ended up. Also, all of the machines are supposed to show "0" ballots cast upon opening. One of our machines did show 1 ballot had been cast on it. We did not use this machine, but we did use all the other machines that had the "elections database" door open. Last but not least, we did not follow the protocol for opening the large cabinets and starting up the machines. In training, I was instructed that all serial numbers on zip ties on doors were to be compared with the serial numbers written down on a form. We did not do this. My Poll Manager said, "I've never seen them not match so we don't need to do this. I can always check it at the end of the day." So, we clipped off all the zip ties with serial numbers without checking them for a match. I also know that the Poll Manager did not check them at the end of the day because I was given the job of putting zip ties on to close up the machines and the Manager was packing up equipment. It as disheartening not to see the security measures followed. Laura Jones [redacted]

- BMDs are easy to hack – demonstrated in federal court and at DEF CON
- Don't need BMDs to be connected to internet – but in GA they *are* connected indirectly
- Don't need extended physical access: voters have enough
- Insiders have more than enough
- Doesn't take a genius
- When margins are small, hacking a few votes/BMDs can change outcomes

Case 1:17-cv-02989-AT Document 1681 Filed 06/14/23 Page 40 of 96

REDACTED VERSION

Figure 9: **ICX USB Interfaces are Exposed to Voters and Unsealed.** A USB cable connects the BMD to an off-the-shelf laser printer. At polling places, the end of the cable attached to the printer is physically accessible to voters, and it is not protected by a tamper-evident seal. Voters could install malware on the ICX by attaching a device to the end of this cable. *Photograph taken by Harri Hursti during polling place observation in Fulton County, November 3, 2020.*

40

- BMDs make voters responsible for cybersecurity
  - most voters don't check printout
  - most who do look for less time than it would take to *count* the contests
  - voters who catch problems can't prove they did
- No way to refute false claims BMDs flipped votes
- If BMDs misbehaved, no way to find correct outcome
- GA doesn't track complaints or spoiled BMD printout (2025 Oakwood muni?)
- GA audits don't check whether QR codes match the text

Election Law Journal: Rules, Politics, and Policy, VOL. 19, NO. 3 | Original Research Articles normal

Ballot-Marking Devices Cannot Ensure the Will of the Voters

Andrew W. Appel, Richard A. DeMillo, and Philip B. Stark

Published Online: 17 Sep 2020 | https://doi.org/10.1089/elj.2019.0619

Tools Share

Abstract

The complexity of U.S. elections usually requires computers to count ballots—but computers can be hacked, so election integrity requires a voting system in which paper ballots can be recounted by hand. However, paper ballots provide no assurance unless they accurately record the votes as expressed by the voters.

Voters can express their intent by indelibly hand-marking ballots or using computers called ballot-marking devices (BMDs). Voters can make mistakes in expressing their intent in either technology, but only BMDs are also subject to hacking, bugs, and misconfiguration of the software that prints the marked ballots. Most voters do not review BMD-printed ballots, and those who do often fail to notice when the printed vote is not what they expressed on the touchscreen. Furthermore, there is no action a voter can take to demonstrate to election officials that a BMD altered their expressed votes, nor is there a corrective action that election officials can take if notified by voters—there is no way to deter, contain, or correct computer hacking in BMDs. These are the essential security flaws of BMDs.

Risk-limiting audits can ensure that the votes recorded on paper ballots are tabulated correctly, but no audit can ensure that the votes on paper are the ones expressed by the voter on a touchscreen: Elections conducted on current BMDs cannot be confirmed by audits. We identify two properties of voting systems, *contestability* and *defensibility*, necessary for audits to confirm election outcomes. No available BMD certified by the Election Assistance Commission is contestable or defensible.

Logic & Accuracy Tests (LAT)

- Designed to check election configuration
- Not designed to detect bugs, malware, hacking
- Utterly inadequate for cybersecurity
- GA LAT doesn't comply w GA law per Judge Totenberg in *Curling*

They May Look and Look, Yet Not See: BMDs Cannot be Tested Adequately

Philip B. Stark[1(✉)] and Ran Xie[2]

[1] University of California, Berkeley, CA, USA
stark@stat.berkeley.edu
[2] Stanford University, Stanford, CA, USA

Abstract. Bugs, misconfiguration, and malware can cause ballot-marking devices (BMDs) to print incorrect votes. Several approaches to testing BMDs have been proposed. In *logic and accuracy testing* (LAT) and *parallel* or *live* testing, auditors input known test votes into the BMD and check whether the printout matches. *Passive* testing monitors the rate at which voters "spoil" BMD printout, on the theory that if BMDs malfunction, the rate will increase noticeably. We provide lower bounds that show that these approaches cannot reliably detect outcome-altering problems, because: (i) The number of possible voter interactions with BMDs is enormous, so testing interactions uniformly at random is hopeless. (ii) To probe the space of interactions intelligently requires an accurate model of voter behavior, but because the space of interactions is so large, building a sufficiently accurate model requires observing an enormous number of voters in every jurisdiction in every election—more voters than there are in most U.S. jurisdictions. (iii) Even with a perfect model of voter behavior, the required number of tests exceeds the number of voters in most U.S. jurisdictions. (iv) An attacker can target interactions that are intrinsically expensive to test, e.g., because they involve voting slowly; or interactions for which tampering is less likely to be noticed, e.g., because the voter uses the audio interface. (v) Whether BMDs misbehave or not, the distribution of spoiled ballots is unknown and varies by election and possibly by ballot style: historical data do not help much. Hence, there is no way to calibrate a threshold for passive testing, e.g., to guarantee at least a 95% chance of noticing that 5% of the votes were altered, with at most a 5% false alarm rate. (vi) Even if the distribution of spoiled ballots were known to be Poisson, the vast majority of jurisdictions do not have enough voters for passive testing to have a large chance of detecting problems but only a small chance of false alarms.

Specific risks of recording votes w/ barcodes & QR codes

- Poor implementations are a vector for hacking
- Sneaky/poor implementations can compromise voter privacy
- Voters can't check what is being counted
- Code might not match human-readable text; happened in PA
- In GA, only the QR code counts unless full hand recount is ordered
- IANAL, but I think this violates HAVA and GA law

Image audits

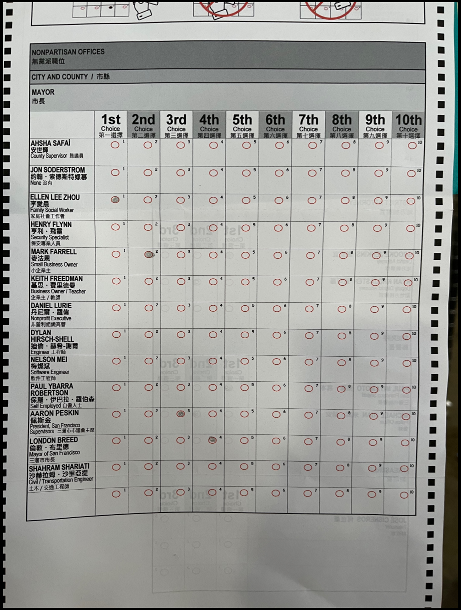
- Can't limit the risk of certifying wrong outcomes
- Images are easy to modify, add, and delete
- Common error to omit a batch or scan a batch more than once – image audit won't catch
- Dominion scans stored low-res b&w: erase some voter marks entirely

UnclearBallot: Automated Ballot Image Manipulation

Matthew Bernhard(✉), Kartikeya Kandula, Jeremy Wink, and J. Alex Halderman

Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, USA
{matber,kartkand,jreremy,jhalderm}@umich.edu

Abstract. As paper ballots and post-election audits gain increased adoption in the United States, election technology vendors are offering products that allow jurisdictions to review ballot images—digital scans produced by optical-scan voting machines—in their post-election audit procedures. Jurisdictions including the state of Maryland rely on such image audits as an alternative to inspecting the physical paper ballots. We show that image audits can be reliably defeated by an attacker who can run malicious code on the voting machines or election management system. Using computer vision techniques, we develop an algorithm that automatically and seamlessly manipulates ballot images, moving voters' marks so that they appear to be votes for the attacker's preferred candidate. Our implementation is compatible with many widely used ballot styles, and we show that it is effective using a large corpus of ballot images from a real election. We also show that the attack can be delivered in the form of a malicious Windows scanner driver, which we test with a scanner that has been certified for use in vote tabulation by the U.S. Election Assistance Commission. These results demonstrate that post-election audits must inspect physical ballots, not merely ballot images, if they are to strongly defend against computer-based attacks on widely used voting systems.

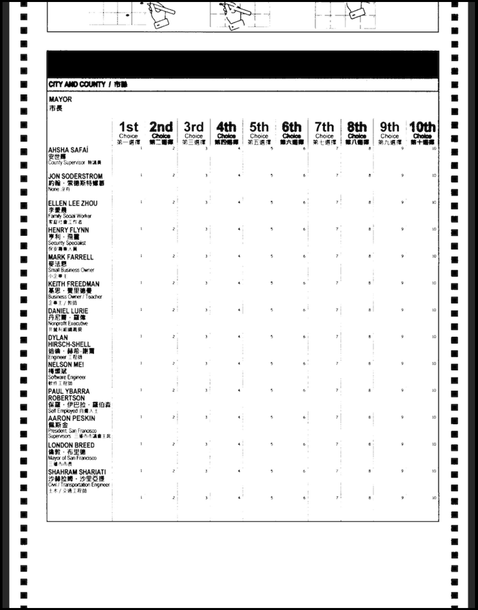


NONPARTISAN OFFICES
無黨派職位

CITY AND COUNTY / 市縣

MAYOR
市長

	1st Choice 第一選擇	2nd Choice 第二選擇	3rd Choice 第三選擇	4th Choice 第四選擇	5th Choice 第五選擇	6th Choice 第六選擇	7th Choice 第七選擇	8th Choice 第八選擇	9th Choice 第九選擇	10th Choice 第十選擇
AHSHA SAFAÍ 安世輝 County Supervisor 縣議員	1	2	3	4	5	6	7	8	9	10
JON SODERSTROM 約翰・索德斯特螺慕 None 沒有	1	2	3	4	5	6	7	8	9	10
ELLEN LEE ZHOU 李愛晨 Family Social Worker 家庭社會工作者	1	2	3	4	5	6	7	8	9	10
HENRY FLYNN 亨利・飛靈 Security Specialist 保安專業人員	1	2	3	4	5	6	7	8	9	10
MARK FARRELL 麥法恩 Small Business Owner 小企業主	1	2	3	4	5	6	7	8	9	10
KEITH FREEDMAN 基思・費里德曼 Business Owner / Teacher 企業主 / 教師	1	2	3	4	5	6	7	8	9	10
DANIEL LURIE 丹尼爾・羅偉 Nonprofit Executive 非營利組織高管	1	2	3	4	5	6	7	8	9	10
DYLAN HIRSCH-SHELL 迪倫・赫希-謝爾 Engineer 工程師	1	2	3	4	5	6	7	8	9	10
NELSON MEI 梅燦斌 Software Engineer 軟件工程師	1	2	3	4	5	6	7	8	9	10
PAUL YBARRA ROBERTSON 保羅・伊巴拉・羅伯森 Self Employed 自僱人士	1	2	3	4	5	6	7	8	9	10
AARON PESKIN 佩斯金 President, San Francisco Supervisors 三藩市市議會主席	1	2	3	4	5	6	7	8	9	10
LONDON BREED 倫敦・布里德 Mayor of San Francisco 三藩市市長	1	2	3	4	5	6	7	8	9	10
SHAHRAM SHARIATI 沙赫拉姆・沙里亞提 Civil / Transportation Engineer 土木 / 交通工程師	1	2	3	4	5	6	7	8	9	10
	1	2	3	4	5	6	7	8	9	10



CITY AND COUNTY / 市縣

MAYOR
市長

	1st Choice 第一選擇	2nd Choice 第二選擇	3rd Choice 第三選擇	4th Choice 第四選擇	5th Choice 第五選擇	6th Choice 第六選擇	7th Choice 第七選擇	8th Choice 第八選擇	9th Choice 第九選擇	10th Choice 第十選擇
AHSHA SAFAÍ 安世輝 County Supervisor 縣議員	1	2	3	4	5	6	7	8	9	10
JON SODERSTROM 約翰・索德斯特螺慕 None 沒有	1	2	3	4	5	6	7	8	9	10
ELLEN LEE ZHOU 李愛晨 Family Social Worker 家庭社會工作者	1	2	3	4	5	6	7	8	9	10
HENRY FLYNN 亨利・飛靈 Security Specialist 保安專業人員	1	2	3	4	5	6	7	8	9	10
MARK FARRELL 麥法恩 Small Business Owner 小企業主	1	2	3	4	5	6	7	8	9	10
KEITH FREEDMAN 基思・費里德曼 Business Owner / Teacher 企業主 / 教師	1	2	3	4	5	6	7	8	9	10
DANIEL LURIE 丹尼爾・羅偉 Nonprofit Executive 非營利組織高管	1	2	3	4	5	6	7	8	9	10
DYLAN HIRSCH-SHELL 迪倫・赫希-謝爾 Engineer 工程師	1	2	3	4	5	6	7	8	9	10
NELSON MEI 梅燦斌 Software Engineer 軟件工程師	1	2	3	4	5	6	7	8	9	10
PAUL YBARRA ROBERTSON 保羅・伊巴拉・羅伯森 Self Employed 自僱人士	1	2	3	4	5	6	7	8	9	10
AARON PESKIN 佩斯金 President, San Francisco Supervisors 三藩市市議會主席	1	2	3	4	5	6	7	8	9	10
LONDON BREED 倫敦・布里德 Mayor of San Francisco 三藩市市長	1	2	3	4	5	6	7	8	9	10
SHAHRAM SHARIATI 沙赫拉姆・沙里亞提 Civil / Transportation Engineer 土木 / 交通工程師	1	2	3	4	5	6	7	8	9	10
	1	2	3	4	5	6	7	8	9	10

2020 recount and “full handcount risk-limiting audit” didn’t prove outcome was right.

Did prove GA’s election procedures are inadequate.

Some counties found thousands of votes that hadn’t been tabulated–were there more?

Count	Election Day			Advance			Absentee by Mail			Provisional		
	Trump	Biden	Jorgensen	Trump	Biden	Jorgensen	Trump	Biden	Jorgensen	Trump	Biden	Jorgensen
Original	193	88	11	1455	1003	23	619	833	15	9	4	1
Recount	162	73	9	1487	1015	25	619	809	15	5	3	1
Audit	243	88	11									

Election day, advance, absentee, and provisional vote tallies for Fulton County, GA, precinct RW01 in the 2020 U.S. Presidential election

	Scanner	Batch	Mode of voting	Trump	Biden	Jorgensen	Write-In	Undervote or blank	Overvote	Image source
1	3	48	absentee	4	93	2	0	0	0	4 at 162
2	2	52	absentee	6	92	0	0	0	0	1 at 1
3	3	12–14	?	12	83	1	0	0	0	4 at 128
4	3	239	?	13	87	0	0	0	0	3 at 177
5	1	80–84	?	118	329	3	2	2	1	3 at 519
6	3	260	absentee	30	66	0	0	0	0	4 at 355
7		AP01A-1	election day	84	62	6	2	1	0	1 at 170
8	3	179–181	absentee	85	224	5	1	2	0	4 at 293
9	2	239	absentee	4	42	0	0	0	0	2 at 153
10	Chastain	12	advance	613	605	24	7	4	0	3 at 351
11	Chastain	114	advance	613	605	24	?	4	0	3 at 270

2020 Fulton County audit board batch sheets that were not entered into the audit results spreadsheet. Including them increases the apparent tabulation error from 634 votes to over 4,569 votes or 0.87 percent, far larger than the statewide margin. https://figshare.com/s/9819e969a8a6172c25bc

pair	Image A	Image B
1	05162_00234_000096	05162_00235_000057
2	05162_00234_000093	05162_00235_000054
3	05162_00234_000074	05162_00235_000036
4	05162_00234_000072	05162_00235_000034
5	05162_00234_000068	05162_00235_000030
6	05162_00234_000069	05162_00235_000031
7	05162_00234_000054	05162_00235_000014
8	05162_00234_000031	05162_00235_000090
9	05162_00234_000026	05162_00235_000085
10	05162_00234_000017	05162_00235_000076
11	05162_00234_000013	05162_00235_000072
12	05162_00234_000014	05162_00235_000073
13	05162_00234_000003	05162_00235_000062
14	05162_00234_000001	05162_00235_000060

Images erroneously included in 1st machine count in Fulton County in 2020 at least twice.
https://figshare.com/s/9819e969a8a6172c25bc

Multiple	Image A	Image B	Image C
1	00801_00044_000168	00801_00043_000168	
2	00801_00044_000083	00801_00043_000083	
3	00801_00044_000042	00801_00043_000042	
4	05160_00074_000023	05160_00067_000008	
5	00794_00017_000024	00791_00026_000091	00791_00019_000010
6	00794_00017_000029	00791_00026_000086	00791_00019_000015
7	00794_00018_000001	00791_00026_000009	00791_00019_000092
8	00794_00018_000011	00791_00026_000019	00791_00019_000082
9	00794_00019_000002	00791_00026_000079	00791_00019_000022
10	00794_00019_000005	00791_00026_000076	00791_00019_000025
11	00794_00019_000006	00791_00026_000075	00791_00019_000026

Images erroneously included in the 2nd Fulton 2020 machine recount at least 2-3 times.

https://figshare.com/s/9819e969a8a6172c25bc

GA's "RLA" charade is hugely wasteful:

- In 2022, "RLA" counted votes on >231,000 cards
- Could have gotten the same evidence from ~1,300 cards using a better RLA strategy
- But this (and image audits) just distracts from the fundamental problem–untrustworthy vote records

Overstatement-Net-Equivalent Risk-Limiting Audit: ONEAudit

Philip B. Stark[1[0000−0002−3771−9604]]

University of California, Berkeley, CA USA stark@stat.berkeley.edu

arXiv:2303.03335v3 [stat.AP] 16 Jun 2023

Abstract. A procedure is a risk-limiting audit (RLA) with risk limit α if it has probability at least $1 - \alpha$ of correcting each wrong reported outcome and never alters correct outcomes. One efficient RLA method, card-level comparison (CLCA), compares human interpretation of individual ballot cards randomly selected from a trustworthy paper trail to the voting system's interpretation of the same cards (cast vote records, CVRs). CLCAs heretofore required a CVR for each cast card and a "link" identifying which CVR is for which card—which many voting systems cannot provide. This paper shows that every set of CVRs that produces the same aggregate results overstates contest margins by the same amount: they are *overstatement-net-equivalent* (ONE). CLCA can therefore use CVRs from the voting system for any number of cards and ONE CVRs created *ad lib* for the rest. In particular:

– Ballot-polling RLA is algebraically equivalent to CLCA using ONE CVRs derived from the overall contest results.
– CLCA can be based on batch-level results (e.g., precinct subtotals) by constructing ONE CVRs for each batch. In contrast to batch-level comparison auditing (BLCA), this avoids manually tabulating entire batches and works even when reporting batches do not correspond to physically identifiable batches of cards, when BLCA is impractical.
– If the voting system can export linked CVRs for only some ballot cards, auditors can still use CLCA by constructing ONE CVRs for the rest of the cards from contest results or batch subtotals.

This works for every social choice function for which there is a known RLA method, including IRV. Sample sizes for BPA and CLCA using ONE CVRs based on contest totals are comparable. With ONE CVRs from batch subtotals, sample sizes are smaller than than for BPA when batches are homogeneous, approaching those of CLCA using CVRs from the voting system, and much smaller than for BLCA: A CLCA of the 2022 presidential election in California at risk limit 5% using ONE CVRs for precinct-level results would sample approximately 70 ballots statewide, if the reported results are accurate, compared to about 26,700 for BLCA. The 2022 Georgia audit tabulated more than 231,000 cards (the expected BLCA sample size was ≈103,000 cards); ONEAudit would have audited ≈1,300 cards. For data from a pilot hybrid RLA in Kalamazoo, MI, in 2018, ONEAudit gives a risk of 2%, substantially lower than the 3.7% measured risk for SUITE, the "hybrid" method the pilot used.

Current RLA methods make it practical to audit every contest in every election. Orange County, CA, has about 1.9 million active voters; Georgia has about 7 million.

TBD (Hrsg.): Proceedings of E-Vote-ID 2023,
2 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 0

Stylish Risk-Limiting Audits in Practice

Amanda K. Glazer[1,2], Jacob V. Spertus[3], Philip B. Stark[4]

Abstract: Risk-limiting audits (RLAs) can use information about which ballot cards contain which contests (*card-style data*, CSD) to ensure that each contest receives adequate scrutiny, without examining more cards than necessary. RLAs using CSD in this way can be substantially more efficient than RLAs that sample indiscriminately from all cast cards. We describe an open-source Python implementation of RLAs using CSD for the Hart InterCivic Verity voting system and the Dominion Democracy Suite® voting system. The software is demonstrated using all 181 contests in the 2020 general election and all 214 contests in the 2022 general election in Orange County, CA, USA, the fifth-largest election jurisdiction in the U.S., with over 1.8 million active voters. (Orange County uses the Hart Verity system.) To audit the 181 contests in 2020 to a risk limit of 5% without using CSD would have required a complete hand tally of all 3,094,308 cast ballot cards. With CSD, the estimated sample size is about 20,100 cards, 0.65% of the cards cast—including one tied contest that required a complete hand count. To audit the 214 contests in 2022 to a risk limit of 5% without using CSD would have required a complete hand tally of all 1,989,416 cast cards. With CSD, the estimated sample size is about 62,250 ballots, 3.1% of cards cast—including three contests with margins below 0.1% and 9 with margins below 0.5%.

GA SoS puts PR above trustworthiness:

- No in-house cybersecurity expertise
- Claimed 2 machine counts and audit in 2020 agreed–but they differ materially
- Claims all differences between hand counts and machine counts are human error (contrary to how RLAs work)–but has never actually checked
- Uses least accurate hand-count method (sort & stack)
- Uses least efficient RLA method (batch-level comparison): more work but not more confidence
- Erroneously claims that auditing one contest proves every contest was decided correctly
- Erroneously claims RLAs show "no votes were flipped"
- Erroneously claimed to J6 Select Committee that no broken seals are ever found

References

Appel, A.W., R. DeMillo, and P.B. Stark, 2020. Ballot-marking devices cannot assure the will of the voters, *Election Law Journal*, *19*:3, 432–450. https://doi.org/10.1089/elj.2019.0619 Preprint: https://www.stat.berkeley.edu/~stark/Preprints/bmd20.pdf

Appel, A.W. and P.B. Stark, 2020. Evidence-Based Elections: Create a Meaningful Paper Trail, Then Audit, *Georgetown Law Technology Review*, *4*, 523–541. https://georgetownlawtechreview.org/wp-content/uploads/2020/07/4.2-p523-541-Appel-Stark.pdf

Bernhard, M., Kandula, K., Wink, J., Halderman, J.A., 2019. UnclearBallot: Automated Ballot Image Manipulation. In: Krimmer, R., et al. Electronic Voting. E-Vote-ID 2019. Lecture Notes in Computer Science, vol 11759. Springer, Cham. https://doi.org/10.1007/978-3-030-30625-0_2

Halderman, J.A. and D. Springall, 2021. Security Analysis of Georgia's ImageCast X Ballot Marking Devices, https://storage.courtlistener.com/recap/gov.uscourts.gand.240678/gov.uscourts.gand.240678.1

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

Stark, P.B., and D.A. Wagner, 2012. Evidence-Based Elections, *IEEE Security and Privacy*, *10*, 33–41. Preprint: https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf

Stark, P.B., and R. Xie, 2022. They may look and look, yet not see: BMDs cannot be tested adequately, *Electronic Voting. E-Vote-ID 2022. Lecture Notes in Computer Science, 13553*, 122–138, Springer-Nature, Cham. https://link.springer.com/chapter/10.1007/978-3-031-15911-4_8

Stark, P.B., 2024. ONEAudit: Overstatement-Net-Equivalent Risk-Limiting Audit, *Proceedings of the 8th Annual Workshop on Advances in Secure Electronic Voting (Voting'23)*, A. Essex et al. (Eds.): FC 2023 Workshops, LNCS 13953, pp. 63–78. 10.1007/978-3-031-48806-1_5 Extended preprint: http://arxiv.org/abs/2303.03335

Stark, P.B., 2024. When Audits and Recounts Distract from Election Integrity: The 2020 U.S. Presidential Election in Georgia, *Proceedings of E-VOTE-ID 2024*, Lecture Notes in Computer Science, in press. Preprint: https://arxiv.org/abs/2408.00055

Stark, P.B., Expert declarations in Curling et al. v. Raffensperger et al. (Northern District of Georgia).
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-1.pdf,
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-2.pdf,
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-3.pdf,
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-4.pdf,
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-5.pdf,
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-6.pdf,
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-7.pdf,
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-8.pdf,
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-9.pdf,
https://www.stat.berkeley.edu/~stark/Preprints/cgg-rept-10.pdf

See https://www.stat.berkeley.edu/~stark/Vote/index.htm for more papers on RLAs, evidence-based elections, etc.