Evidence-Based Elections

Santa Fe Institute

Philip B. Stark

27 January 2021

University of California, Berkeley

Many collaborators including (most recently) Andrew Appel, Josh Benaloh, Matt Bernhard, Michelle Blom, Andrew Conway, Rich DeMillo, Steve Evans, Amanda Glazer, Alex Halderman, Mark Lindeman, Kellie Ottoboni, Eddie Perez, Ron Rivest, Peter Ryan, Jake Spertus, Peter Stuckey, Vanessa Teague, Poorvi Vora

Berkeley News

Research ▾ People ▾ Campus & community

POLITICS & SOCIETY, RESEARCH

Is Trump right about Georgia vote?

By Robert Sanders, Media relations | NOVEMBER 13, 2020

Tweet Share 388 Email Print

POLITICS ELECTION 2020 GEORGIA

Why Georgia's Unscientific Recount 'Horrified' Experts

Observers, including the inventor of the auditing process used by the state, were skeptical of a measure seemingly aimed at placating the GOP.

By Timothy Pratt

NOVEMBER 20, 2020

#Giuliani #Georgia #Hearing

LIVE: Giuliani Testifies—Georgia Senate Subcommittee Continues Hearing on Election Issues (Dec. 30)

883,360 views • Streamed live on Dec 30, 2020

45K 952 SHARE SAVE

WSB-TV 2 ATLANTA

Watch Live Weather COVID-19 Vaccine News Video Coronavirus Traffic Com

Trump supporters file lawsuit asking Georgia to decertify election, declare Trump the winner

Sidney Powell files voting lawsuit in Ga.

Sidney Powell shares 270-page binder of documents buttressing election fraud claims

by Daniel Chaitin, Breaking News Editor | | December 27, 2020 08:56 PM
| *Updated Dec 27, 2020, 10:33 PM*

FIFTH SUPPLEMENTAL DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my declarations of September 9, 2018, September 30, 2018, October 22, 2019, and December 16, 2019. I stand by everything in the previous declarations.

I. False Assertions about the Fulton County Pilot Audit

2. Secretary of State Raffensperger issued the following (undated) press release on approximately June 30, 2020:[1]

> AUDIT SUPPORTS PRIMARY OUTCOME
>
> **(ATLANTA)** – A pilot post-election audit Monday confirmed the outcomes of the presidential preference primaries in Fulton County, Secretary of State Brad Raffensperger announced today.
>
> "This procedure demonstrates once again the validity of the results produced by Georgia's new secure paper-ballot system," [SOS Raffensperger] said. "Auditing

[1] https://sos.ga.gov/index.php/general/audit_supports_primary_outcome last visited 27 July 2020.

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

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

FIFTH SUPPLEMENTAL DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my declarations of September 9, 2018, September 30, 2018, October 22, 2019, and December 16, 2019. I stand by everything in the previous declarations.

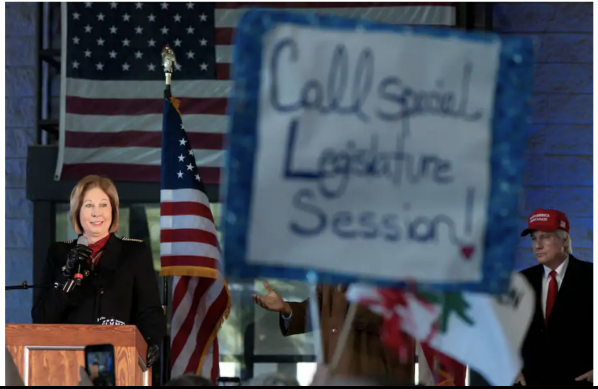
I. False Assertions about the Fulton County Pilot Audit

2. Secretary of State Raffensperger issued the following (undated) press release on approximately June 30, 2020:[1]

> AUDIT SUPPORTS PRIMARY OUTCOME
>
> **(ATLANTA)** – A pilot post-election audit Monday confirmed the outcomes of the presidential preference primaries in Fulton County, Secretary of State Brad Raffensperger announced today.
>
> "This procedure demonstrates once again the validity of the results produced by Georgia's new secure paper-ballot system," [SOS Raffensperger] said. "Auditing

[1] https://sos.ga.gov/index.php/general/audit_supports_primary_outcome last visited 27 July 2020.

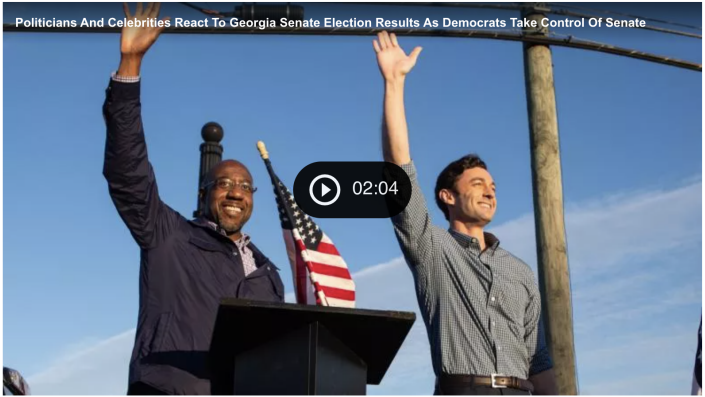
Sidney Powell's secret 'military intelligence expert,' key to fraud claims in election lawsuits, never worked in military intelligence



Newsweek

Sidney Powell Drops Georgia Suit, Marking End to Presidential Election-Related Lawsuits in State

BY NICOLE FALLERT ON 1/19/21 AT 5:00 PM EST



SHARE

Reuters)

Politics

Dominion sues Giuliani over false election fraud claims

January 26, 2021 | 12:51 PM PST

Voting machine company Dominion filed a $1.3 billion lawsuit against former president Donald Trump's lawyer Rudy Giuliani on Jan. 25.

Related

Giuliani wasn't just a Trump partisan but a shrewd marketer of vitamins, gold, lawsuit says

Politics

Dominion sues pro-Trump lawyer Sidney Powell, seeking more than $1.3 billion

Elections Should be Grounded in Evidence, Not Blind Trust

COMMENTARY Philip B. Stark, Edward Perez, and J. Alex Halderman Jan. 4, 2021 9:15 am ET O

Text size

Georgia Democratic Senate candidate Raphael Warnock speaks during a drive-in rally on Jan. 3, 2021 in Savannah. Michael M. Santiago/Getty Images

President Donald Trump's attempt to pressure Georgia election officials to "find" votes he didn't win is keeping election integrity in the spotlight. Tomorrow's Senate runoffs will determine which party controls the chamber, and there's a high likelihood that this round of voting will also be declared illegitimate by the losers. Even though there is no compelling evidence the 2020 vote was rigged, U.S. elections are insufficiently equipped to counter such claims because of a flaw in American voting. The way we conduct elections does not routinely produce public evidence that outcomes are correct.

- Voters hand-mark paper ballots to create a trustworthy, durable paper vote record. Voters who cannot hand-mark a ballot independently are provided assistive technologies, such as electronic ballot marking devices. But because these devices are subject to hacking, bugs, and software misconfiguration, the use of such ballot-marking devices should be limited.
- Election officials protect the paper ballots to ensure no ballot has been added, removed, or altered. This requires stringent physical security protocols and ballot accounting, among other things.
- Election officials count the votes, using technology if they choose. If the technology altered the outcome, that will (with high confidence) be corrected by the steps below.
- Election officials reconcile and verify the number of ballots and the number of voters, with a complete canvass to ensure that every validly cast ballot is included in the count.
- Election officials check whether the paper trail is trustworthy using a transparent "compliance audit," reviewing chain-of-custody logs and security video, verifying voter eligibility, reconciling numbers of ballots of each style against poll book signatures and other records, and accounting for every ballot that was issued.
- Election officials check the results with an audit that has a known, large probability of catching and correcting wrong reported outcomes—and no chance of altering correct outcomes. The inventory of paper ballots used in the audit must be complete and the audit must inspect the original hand-marked ballots, not images or copies.

None of these steps stands alone. An unexamined set of paper ballots, no matter how trustworthy, provides no evidence. Conversely, no matter how rigorous, audits and recounts of an untrustworthy paper trail provide no evidence that the reported winners won. Auditing or recounting machine-marked ballots or hand-marked ballots that have not been kept secure can check whether the reported outcome reflects *that paper trail*, but cannot provide evidence that the reported winners won.

Arguments that US elections can't be hacked:

- Physical security
- Not connected to the Internet
- Tested before election day
- Too decentralized
- Paper

Arguments that US elections can't be hacked:

- Physical security
  - "sleepovers," unattended equipment in warehouses, school gyms, ...
  - locks use minibar keys
  - bad/no seal protocols, easily defeated seals
  - no routine scrutiny of custody logs, 2-person custody rules, ...
- Not connected to the Internet
- Tested before election day
- Too decentralized

Arguments that US elections can't be hacked:

- Physical security
- Not connected to the Internet
  - remote desktop software
  - wifi, bluetooth, cellular modems, ... https://tinyurl.com/r8cseun
  - removable media used to configure equipment & transport results
    - Zip drives
    - USB drives. Stuxnet, anyone?
  - parts from foreign manufacturers, including China; Chinese pop songs in flash
- Tested before election day
- Too decentralized
- Paper

The New York Times

Russia Targeted Election Systems in All 50 States, Report Finds

A voter casting his ballot in the midterm elections last year in Medina, N.D. Hilary Swift for The New York Times

By David E. Sanger and Catie Edmondson

July 25, 2019

716

WASHINGTON — The Senate Intelligence Committee concluded Thursday that election systems in all 50 states were targeted by Russia in 2016, an

Remote Access Statement | Election Systems & Software

https://essvote.com/media-center/press-statements/remote-access-statement/

ES&S voting machines across the nation do not have any form of **remote access** capability. **ES&S** has never **installed** remote connection **software** on any vote ...

Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States

Remote-access software and modems on election equipment 'is the worst decision for security short of leaving ballot boxes on a Moscow street corner.'

By **Kim Zetter**

Jul 17 2018, 5:00am Share Tweet Snap

IMAGE: SHUTTERSTOCK

The nation's top voting machine maker has admitted in a letter to a federal lawmaker that the company installed remote-access software on election-management systems it sold over a period of six years, raising questions about the security of those systems and the integrity of elections that were conducted with them.

In a letter sent to Sen. Ron Wyden (D-OR) in April and obtained recently by Motherboard, Election Systems and Software acknowledged that it had "provided pcAnywhere remote connection software ... to a small number of customers between 2000 and 2006," which was installed on the election-management system ES&S sold them.

CYBERSECURITY

Election commission orders top voting machine vendor to correct misleading claims

This isn't the first time Election Systems & Software has faced accusations of making fabricated or misleading assertions about its voting machines.

A voter in a voting booth. | Steve Helber/AP Photo

By KIM ZETTER
08/13/2020 05:00 PM EDT

The federal Election Assistance Commission has rebuked the nation's top voting-machine maker over marketing materials that the panel says deceptively implied the company's voting machines are EAC-certified.

Voting Machine Hacking Village

Report on Cyber Vulnerabilities in

U.S. Election Equipment, Databases, and Infrastructure

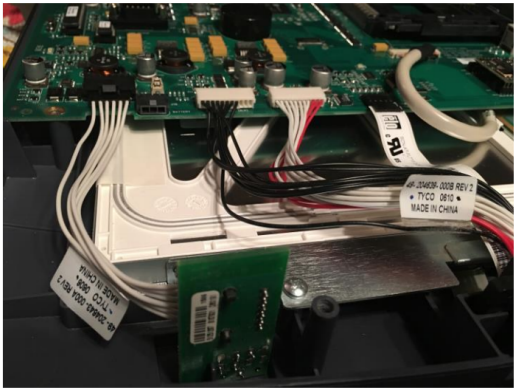
September 2017

Co-authored by:
Matt Blaze, University of Pennsylvania
Jake Braun, University of Chicago & Cambridge Global Advisors
Harri Hursti, Nordic Innovation Labs
Joseph Lorenzo Hall, Center for Democracy & Technology
Margaret MacAlpine, Nordic Innovation Labs
Jeff Moss, DEFCON

The results were sobering. **By the end of the conference, every piece of equipment in the Voting Village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources were quite capable of undermining the confidentiality, integrity, and availability of these systems**, including:

- The first voting machine to fall – an AVS WinVote model – was hacked and taken control of remotely in a matter of minutes, using a vulnerability from 2003, meaning that for the entire time this machine was used from 2003-2014 it could be completely controlled remotely, allowing changing votes, observing who voters voted for, and shutting down the system or otherwise incapacitating it.
- That same machine was found to have an unchangeable, universal default password – found with a simple Google search – of "admin" and "abcde."
- An "electronic poll book", the Diebold ExpressPoll 5000, used to check in voters at the polls, was found to have been improperly decommissioned with live voter file data still on the system; this data

Moreover, a closer physical examination of the machines found, as expected, multiple cases of foreign-manufactured internal parts (including hardware developed in China), highlighting the serious possibility of supply chain vulnerabilities. This discovery means that a hacker's point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line. With an ability to infiltrate voting infrastructure at any point in the supply chain process, then the ability to synchronize and inflict large-scale damage becomes a real possibility. Also, as expected, many of these systems had extensive use of binary software for subcomponents that could completely control the behavior of the system and information flow, highlighting the need for greater use of trusted computing elements to limit the effect of malicious software. In other words, a nation-state actor with resources, expertise and motive – like Russia – could exploit these supply chain security flaws to plant malware into the parts of every machine, and indeed could breach vast segments of U.S. election infrastructure remotely, all at once.



DEF CON 27 Voting Village Report!

Posted 9.26.19

The DEF CON Voting Village has released its findings from DEF CON 27!

This is the third year we've hosted the Voting Village, and this year we were able to give attendees access to over 100 machines, all of which are currently certified for use in at least one US jurisdiction. The units tested included direct-recording electronic (DRE) voting machines, electronic poll books, Ballot Marking Devices (BMDs), Optical scanners and Hybrid systems.

The hackers at DEF CON once again compromised every single machine over the 2.5 day event, many of them with trivial attacks that require no sophistication or special knowledge on the part of the attacker. In too many cases

APAC SEPTEMBER 23, 2020 / 5:52 PM / UPDATED 2 HOURS AGO

Software vendor Tyler Technologies tells U.S. local government clients it was hacked

By Joseph Menn 3 MIN READ

SAN FRANCISCO (Reuters) - Tyler Technologies TYL.N, whose products are used by U.S. states and counties to share election data, said on Wednesday that an unknown party had hacked its internal systems.

Tyler, whose platforms are used by elections officials to display voting results, among other tasks, confirmed the breach in an email to Reuters after warning clients in an email earlier in the day.


D-Suite 5.5 EAC
DOMINION VOTING
DELL
ICC01
Tabulator 950
D-Suite 5.5 EAC
DOMINION VOTING
DELL


Activation Codes Export
People
Photos
S
Settings
Skype
Spotify Music
Sticky Notes
T
Tips
V
Video Editor
Voice Recorder
W
Weather
Windows Accessories
Windows Administrative Tools
Windows Defender Security Center
Windows Ease of Access
Wednesday
2
See all your mail in one place
And more...
Mail
My Office
OneNote
Explore
Microsoft Store
Microsoft Edge
Weather
Spotify Music
Skype
Microsoft News
Fitbit Coach
ACG Player
Xbox Con...
Photos
FRIENDS
Microsoft Solitaire Collection
ASPHALT 8 AIRBORNE
Seekers Notes...

Arguments that US elections can't be hacked:

- Physical security
- Not connected to the Internet
- Tested before election day
  - Dieselgate, anyone?
  - Northampton, PA
  - Los Angeles, CA VSAP
- Too decentralized
- Paper

Expensive, Glitchy Voting Machines Expose 2020 Hacking Risks

Paper ballots may be safer and cheaper, but local officials swoon at digital equipment.

By Kartikay Mehrotra and Margaret Newkirk
November 8, 2019, 12:30 PM PST

A man casts his ballot at polling station in New Jersey in 2016. *Photographer: Eduardo Munoz Alvarez/AFP via Getty Images*

The first sign something was wrong with Northampton County, Pennsylvania's state-of-the-art voting system came on Election Day when a voter called the local Democratic Party chairman to say a touchscreen in her precinct was acting "finicky." As she scrolled down the ballot, the tick-marks next to candidates she'd selected kept disappearing.

(Bloomberg) -- The first sign something was wrong with Northampton County, Pennsylvania's state-of-the-art voting system came on Election Day when a voter called the local Democratic Party chairman to say a touchscreen in her precinct was acting "finicky." As she scrolled down the ballot, the tick-marks next to candidates she'd selected kept disappearing.

Her experience Nov. 5 was no isolated glitch. Over the course of the day, the new election machinery, bought over the objections of cybersecurity experts, continued to malfunction. Built by Election Systems & Software, the ExpressVote XL was designed to marry touchscreen technology with a paper-trail for post-election audits. Instead, it created such chaos that poll workers had to crack open the machines, remove the ballot records and use scanners summoned from across state lines to conduct a recount that lasted until 5 a.m.

In one case, it turned out a candidate that the XL showed getting just 15 votes had won by about 1,000. Neither Northampton nor ES&S know what went wrong.

In Philadelphia, a three-person election commission discounted cybersecurity warnings and, in February, selected ExpressVote XL from ES&S after a massive lobbying effort. It has a 32-inch touchscreen at a cost of $29 million, or $27.59 per voter, not including roughly $3.8 million over 10 years in fees.

But the decision raised suspicions. State Auditor General Eugene DePasquale noted that the request for proposals appeared to favor equipment of the XL's type and size. An investigation by City Controller Rebecca Rhynhart later found that ES&S had courted the tiny commission for six years, spending almost half a million dollars lobbying it. The company paid a $2.9 million penalty—the highest in Philadelphia history—for failing to disclose lobbying on bid documents, according to the city controller's office.

2020 ELECTIONS

Los Angeles County's risky voting experiment

The nation's most populous county is debuting new voting technology that has drawn scrutiny.

By KIM ZETTER
03/03/2020 04:30 AM EST

In November 2018, potential voters wait in long lines to register and vote at the Los Angeles County Registrar's office. | Mark J. Terrill, File/AP Photo

Los Angeles County spent nine years working on a government-designed and -owned voting system with the goal of setting a new standard for security, reliability and transparency.

Instead, millions of county voters on Super Tuesday will cast ballots on a system in which numerous security flaws were found. This has prompted some election integrity experts to call for barring the system from elections until they're fully resolved. The issues include multiple digital and physical vulnerabilities, some of them identified in a recent assessment by California's secretary of state and others identified by outside computer security

nty-voting...

The judge opens the sale of Scytl and awaits offers for the company until June 22

June 7, 2020

Arguments that US elections can't be hacked:

- Physical security
- Not connected to the Internet
- Tested before election day
- Too decentralized
  - market concentrated: few vendors/models in use
  - vendors & EAC have been hacked
  - demonstration viruses that propagate across voting equipment
  - "mom & pop" contractors program thousands of machines, no IT security
  - changing presidential race requires changing votes in only a few counties
  - primary contractor for reporting is foreign, bankrupt
  - many weak links

Paper

- Some claim all's well because of "paper backups"
- But paper by itself does nothing.
- How paper is marked, curated, tabulated, & audited are crucial.

Security properties of paper

- tangible/accountable
- tamper evident
- human readable
- large alteration/substitution attacks require physical access & many accomplices

Security properties of paper

- tangible/accountable
- tamper evident
- human readable
- large alteration/substitution attacks require physical access & many accomplices

Not all paper is trustworthy

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

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

SEVENTH DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my declarations of September 9, 2018; September 30, 2018; October 22, 2019; December 16, 2019; August 23, 2020; and August 31, 2020. I stand by everything in the previous declarations.
2. In his testimony on 11 September 2020, Defendant's expert Dr. Ben Adida made a

Mother Jones

Smart, Fear

POLITICS ENVIRONMENT CRIME AND JUSTICE FOOD MEDIA INVESTIGATIONS PHO

POLITICS JANUARY 8, 2020

A New Voting System Promises Reliable Paper Records. Security Experts Warn It Can't Be Trusted.

A just-released study says over ninety percent of errors introduced by ballot marking devices go undetected.

AJ VICENS
Reporter
Bio | Follow

FREEDOM TO TINKER
research and expert commentary on digital technologies in public life

Serious design flaw in ESS ExpressVote touchscreen: "permission to cheat"

SEPTEMBER 14, 2018 BY ANDREW APPEL

Kansas, Delaware, and New Jersey are in the process of purchasing voting machines with a serious design flaw, and they should reconsider while there is still time!

Over the past 15 years, almost all the states have moved away from paperless touchscreen voting systems (DREs) to optical-scan paper ballots. They've done so because if a paperless touchscreen is hacked to give fraudulent results, there's no way to know and no way to correct; but if an optical scanner were hacked to give fraudulent results, the fraud could be detected by a random audit *of the paper ballots that the voters actually marked*, and corrected by a recount of those paper ballots.

Washington MONTHLY

Donald Trump's Favorite Voting Machines

Ballot-marking devices in key swing states could give him the perfect excuse to contest the election

by Art Levine September 23, 2020 POLITICS

Accepted for publication in *Election Law Journal*

Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters

Andrew W. Appel[†]
Princeton University

Richard A. DeMillo[†]
Georgia Tech

Philip B. Stark[†]
Univ. of California, Berkeley

February 14, 2020

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 device (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.

Testing Cannot Tell Whether Ballot-Marking Devices Alter Election Outcomes

Philip B. Stark and Ran Xie

[1] University of California, Berkeley
[2] University of California, Berkeley

29 July 2020

Abstract. Like all computerized systems, ballot-marking devices (BMDs) can be hacked, misprogrammed, and misconfigured. BMD printout might not reflect what the BMD screen or audio conveyed to the voter. If voters complain that BMDs misbehaved, officials have no way to tell whether BMDs malfunctioned, the voters erred, or the voters are attempting to cast doubt on the election. Several approaches to testing BMDs have been proposed. In pre-election *logic and accuracy* (*L&A*) tests, trusted agents input known test patterns into the BMD and check whether the printout matches. In *parallel* or *live* testing, trusted agents use the BMDs on election day, emulating voters. In *passive* testing, trusted agents monitor the rate at which voters "spoil" ballots and request another opportunity to mark a ballot: an anomalously high rate might result from BMD malfunctions. In practice, none of these methods can protect against outcome-altering problems. L&A testing is ineffective against malware in part because BMDs "know" the time and date of the test and the election. Neither L&A nor parallel testing can probe even a small fraction of the combinations of voter preferences, device settings, ballot language, duration of voter interaction, input and output interfaces, and other variables that could comprise enough votes to change outcomes. Under mild assumptions, to develop a model of voter interactions with BMDs accurate enough to ensure that parallel tests could reliably detect changes to 5% of the votes (which could change margins by 10% or more) would require monitoring the behavior of more than a million voters in each jurisdiction in minute detail—but the median turnout by jurisdiction in the U.S. is under 3000 voters, and 2/3 of U.S. jurisdictions have fewer than 43,000 active voters. Moreover, all voter privacy would be lost. Given an accurate model of voter behavior, the number of tests required is still larger than the turnout in a typical U.S. jurisdiction. Even if less testing sufficed, it would require extra BMDs, new infrastructure for creating test interactions and reporting test results, additional polling-place staff, and more training. Under optimistic assumptions, passive testing that has a 99% chance of detecting a 1% change to the margin with a 1% false alarm rate is impossible in jurisdictions with fewer than about 1 million voters, even if the "normal" spoiled ballot rate were known exactly and did not vary from election to election and place to place. Passive testing would also require training and infrastructure to monitor the spoiled ballot rate in real time. And if parallel or passive testing discovers a problem, the only remedy is a new election: there is no way to reconstruct the correct election result from an untrustworthy paper trail. Minimizing the number of votes cast using BMDs is prudent election administration.

- Hand-marked paper ballots are a record of what the voter did.
- Machine-marked paper ballots are a record of what the machine did.
- BMDs make voters responsible for catching & correcting machine errors/bugs/hacks
- Few voters notice errors in BMD printout

Did the reported winner really win?

- Procedure-based vs. evidence-based elections
  - sterile scalpel v. patient's condition

Did the reported winner really win?

- Procedure-based vs. evidence-based elections
  - sterile scalpel v. patient's condition
- *Any* way of counting votes can make mistakes
- *Every* electronic system is vulnerable to bugs, configuration errors, & hacking
- **Did error/bugs/hacking cause losing candidate(s) to appear to win?**
- Minimum accuracy standard: find who really won.

Voting system properties needed to justify public trust

- (Strong) Software Independence
- Contestability
- Defensibility

Voting system properties needed to justify public trust

- (Strong) Software Independence
- Contestability
- Defensibility

DREs, BMDs, online voting are none of the above.

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.**

I. Introduction

IDEALLY, what should an election do? Certainly, an election should find out who won, but we believe it also should produce convincing evidence that it found the real winners—or report that it cannot. This is not automatic; it requires thoughtful design of voting equipment, carefully planned and implemented voting and vote counting processes, and rigorous post-election auditing.

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, North Carolina irretrievably lost 4,400 votes; other machines in Mecklenburg, North Carolina recorded 3,955 more votes than the number of people who voted; in Bernalillo County, New Mexico, machines recorded 2,700 more votes than voters; in Mahoning County, Ohio, some machines reported a negative total vote count; and in Fairfax, Virginia, county officials found that for every hundred or so votes cast for one candidate, the electronic voting machines subtracted one vote for her [2]. In short, when elections are conducted on paperless voting

Risk-Limiting Audits (RLAs, Stark, 2008)

- **If there's a trustworthy paper record of votes, can check whether reported winner really won.**
- If you accept a controlled "risk" of not correcting the reported outcome if it is wrong, typically don't need to look at many ballots if outcome is right.

A risk-limiting audit has a known minimum chance of correcting the reported outcome if the reported outcome is wrong (& doesn't alter correct outcomes).

A risk-limiting audit has a known minimum chance of correcting the reported outcome if the reported outcome is wrong (& doesn't alter correct outcomes).

Risk limit: largest possible chance of *not* correcting reported outcome, if reported outcome is wrong.

A risk-limiting audit has a known minimum chance of correcting the reported outcome if the reported outcome is wrong (& doesn't alter correct outcomes).

Risk limit: largest possible chance of *not* correcting reported outcome, if reported outcome is wrong.

Wrong means accurate handcount of *trustworthy* paper would find different winner(s).

A risk-limiting audit has a known minimum chance of correcting the reported outcome if the reported outcome is wrong (& doesn't alter correct outcomes).

Risk limit: largest possible chance of *not* correcting reported outcome, if reported outcome is wrong.

Wrong means accurate handcount of *trustworthy* paper would find different winner(s).

Establishing whether paper trail is trustworthy involves other processes, generically, *compliance audits*

RLA pseudo-algorithm

```
while (!(full handcount) && !(strong evidence outcome is correct)) {
    examine more ballots
}
```

RLA pseudo-algorithm

```
while (!(full handcount) && !(strong evidence outcome is correct)) {
    examine more ballots
}

if (full handcount) {
    handcount result is final
}
```

The National Academies of SCIENCES ENGINEERING MEDICINE

Home

Elections should be conducted with human-readable paper ballots. Paper ballots form a body of evidence that is not subject to manipulation by faulty software or hardware and that can be used to audit and verify the results of an election. Human-readable paper ballots may be marked by hand or by machine (using a ballot-marking device), and they may be counted by hand or by machine (using an optical scanner), the report says. Voters should have an opportunity to review and confirm their selections before depositing the ballot for tabulation. Voting machines that do not provide the capacity for independent auditing – i.e., machines that do not produce a printout of a voter's selections that can be verified by the voter and used in audits – should be removed from service as soon as possible.

States should mandate a specific type of audit known as a "risk-limiting" audit prior to the certification of election results. By examining a statistically appropriate random sample of paper ballots, risk-limiting audits can determine with a high level of confidence whether a reported election outcome reflects a correct tabulation

Risk-Limiting Audits

- Endorsed by NASEM, PCEA, ASA, LWV, CC, VV, ...
- ~60 pilot audits in AK, CA, CO, GA, IN, KS, MI, MT, NJ, OH, OR, PA, RI, WA, WY, VA, DK.
- CA counties: Alameda, El Dorado, Humboldt, Inyo, Madera, Marin, Merced, Monterey, Napa, Orange, San Francisco, San Luis Obispo, Santa Clara, Santa Cruz, Stanislaus, Ventura, Yolo.
- Routine statewide in CO since 2017. Statewide audits in AK, KS, WY in 2020.
- Laws in CA, CO, RI, VA, WA

Role of math/stat

- Reduce workload!
- Get evidence about the population of cast ballots from a random sample.
- Guarantee a large chance of correcting wrong outcomes; minimize work if the outcome is correct.
- When can you stop inspecting ballots?
  - When there's strong evidence that a full hand count is pointless

RLA as a hypothesis test

- Null hypothesis: reported outcome is *wrong*.
- Significance level (Type I error rate) is "risk"
- Frame the hypothesis quantitatively: necessary and sufficient conditions

b_i is ith ballot card, N cards in all.

$$1_{\text{candidate}}(b_i) \equiv \begin{cases} 1, & \text{ballot } i \text{ has a mark for candidate} \\ 0, & \text{otherwise.} \end{cases}$$

$$A_{\text{Alice,Bob}}(b_i) \equiv \frac{1_{\text{Alice}}(b_i) - 1_{\text{Bob}}(b_i) + 1}{2} \geq 0.$$

mark for Alice but not Bob, $A_{\text{Alice,Bob}}(b_i) = 1$.

mark for Bob but not Alice, $A_{\text{Alice,Bob}}(b_i) = 0$.

marks for both (overvote) or neither (undervote) or doesn't contain contest, $A_{\text{Alice,Bob}}(b_i) = 1/2$.

$$\bar{A}^{b}_{\mathrm{Alice,Bob}} \equiv \frac{1}{N} \sum_{i=1}^{N} A_{\mathrm{Alice,Bob}}(b_i).$$

Mean of a finite nonnegative list of N numbers.

Alice won iff $\bar{A}^{b}_{\mathrm{Alice,Bob}} > 1/2$.

Plurality & Approval Voting

$K \geq 1$ winners, $C > K$ candidates in all.

Candidates $\{w_k\}_{k=1}^{K}$ are reported winners.

Candidates $\{\ell_j\}_{j=1}^{C-K}$ reported losers.

Plurality & Approval Voting

$K \geq 1$ winners, $C > K$ candidates in all.

Candidates $\{w_k\}_{k=1}^{K}$ are reported winners.

Candidates $\{\ell_j\}_{j=1}^{C-K}$ reported losers.

Outcome correct iff

$$\bar{A}^{b}_{\mathrm{w_k},\ell_\mathrm{j}} > 1/2, \quad \text{for all } 1 \leq k \leq K, \;\; 1 \leq j \leq C-K$$

$K(C-K)$ inequalities.

Plurality & Approval Voting

$K \geq 1$ winners, $C > K$ candidates in all.

Candidates $\{w_k\}_{k=1}^{K}$ are reported winners.

Candidates $\{\ell_j\}_{j=1}^{C-K}$ reported losers.

Outcome correct iff

$$\bar{A}^{b}_{\mathrm{w_k},\ell_\mathrm{j}} > 1/2, \quad \text{for all } 1 \leq k \leq K, \;\; 1 \leq j \leq C - K$$

$K(C - K)$ inequalities.

Same approach works for D'Hondt & other proportional representation schemes. (Stark & Teague 2015)

Super-majority

$f \in (1/2, 1]$.

Alice won iff

$$(\text{votes for Alice}) > f \times ((\text{valid votes for Alice}) + (\text{valid votes for everyone else}))$$

Set

$$A(b_i) \equiv \begin{cases} \frac{1}{2f}, & b_i \text{ has a mark for Alice and no one else} \\ 0, & b_i \text{ has a mark for exactly one candidate, not Alice} \\ \frac{1}{2}, & \text{otherwise.} \end{cases}$$

Alice won iff

$$\bar{A}^b > 1/2.$$

Borda count, STAR-Voting, & other additive weighted schemes

Winner is the candidate who gets most "points" in total.

$s_{\text{Alice}}(b_i)$: Alice's score on ballot i.

$s_{\text{cand}}(b_i)$: another candidate's score on ballot i.

s^+: upper bound on the score any candidate can get on a ballot.

Alice beat the other candidate iff Alice's total score is bigger than theirs:

$$A_{\text{Alice,c}}(b_i) \equiv \frac{s_{\text{Alice}}(b_i) - s_{\text{c}}(b_i) + s^+}{2s^+}.$$

Alice won iff $\bar{A}^b_{\text{Alice,c}} > 1/2$ for every other candidate c.

Ranked-Choice Voting, Instant-Runoff Voting (RCV/IRV)

2 types of assertions together give sufficient (not necessary) conditions (Blom et al. 2018):

1. Candidate i has more first-place ranks than candidate j has total mentions.
2. After a set of candidates E have been eliminated from consideration, candidate i is ranked higher than candidate j on more ballots than *vice versa*.

Both can be written $\bar{A}^b > 1/2$.

Finite set of such assertions implies reported outcome is right.

More than one set suffices; can optimize expected workload.

Auditing assertions

Test *complementary null hypothesis* $\bar{A}^b \leq 1/2$ sequentially.

- Audit until either all complementary null hypotheses about a contest are rejected at significance level α or until all ballots have been tabulated by hand.
- Yields a RLA of the contest in question at risk limit α.
- No multiplicity adjustment needed.

Sequential testing originated w/ Wald (1945; military secret before).

Key object: martingale.

Sequence of rvs $\{Z_j\}$ s.t.

- $\mathbb{E}|Z_j| < \infty$
- $\mathbb{E}(Z_{j+1}|Z_1, \ldots, Z_j) = Z_j$

Kolmogorov's/Ville's inequality

If $\{Z_j\}$ is a nonnegative martingale, then for any $p > 0$ and all $J \in \{1, \ldots, N\}$,

$$\Pr\left(\max_{1 \le j \le J} Z_j(t) > 1/p\right) \le p\, \mathbb{E}|Z_J|.$$

Markov's inequality applied to optionally stopped martingales.

Wald's SPRT

For $j = 1, 2, \ldots$, let P_{j0} be the probability of $X_1, \ldots, X_j$ under H_0; P_{j1} be the probability of $X_1, \ldots, X_j$ under H_1.

$$Z_j = \frac{P_{j1}}{P_{j0}}, \quad j = 1, 2, \ldots$$

is a nonnegative martingale if H_0 is true.

$1/Z_j$ is a valid P-value for H_0 at step j.

Ballot-polling audits

Sample sequentially w/o replacement from a finite population of N non-negative items, $\{x_1, \ldots, x_N\}$, with $x_j \geq 0$, $\forall j$.

Total is $N\bar{x} \geq 0$. Value of the jth item drawn is X_j.

If $\bar{x} = t$, $\mathbb{E}X_1 = t$, so $\mathbb{E}(X_1/t) = 1$.

Given $X_1, \ldots, X_n$, the total of the remaining $N - n$ items is $Nt - \sum_{j=1}^{n} X_j$, so the mean of the remaining items is

$$\frac{Nt - \sum_{j=1}^{n} X_j}{N - n} = \frac{t - \frac{1}{N}\sum_{j=1}^{n} X_j}{1 - n/N}.$$

Define

$$Y_1(t) \equiv \begin{cases} X_1/t, & Nt > 0, \\ 1, & Nt = 0, \end{cases}$$

and for $1 \leq n \leq N-1$,

$$Y_{n+1}(t) \equiv \begin{cases} X_{n+1} \frac{1-\frac{n}{N}}{t-\frac{1}{N}\sum_{j=1}^{n} X_j}, & \sum_{j=1}^{n} X_j < Nt, \\ 1, & \sum_{j=1}^{n} X_j \geq Nt. \end{cases}$$

Then $\mathbb{E}(Y_{n+1}(t)|Y_1, \ldots Y_n) = 1$.

Let $Z_n(t) \equiv \prod_{j=1}^{n} Y_j(t)$.

$\mathbb{E}|Z_k| \leq \max_j x_j < \infty$ and

$$\mathbb{E}\left(Z_{n+1}(t)|Z_1(t), \ldots Z_n(t)\right) = \mathbb{E}\left(Y_{n+1}(t)Z_n(t)|Z_1(t), \ldots Z_n(t)\right) = Z_n(t).$$

Thus

$$(Z_1(t), Z_2(t), \ \ldots, Z_N(t))$$

is a non-negative closed martingale.

Thus a P-value for the hypothesis $\bar{x} = t$ for data $X_1, \ldots X_J$ is $\left(\max_{1 \leq j \leq J} Z_j(t)\right)^{-1} \wedge 1$.

Kaplan's martingale (KMART)

Let $S_j \equiv \sum_{k=1}^{j} X_k$, $\tilde{S}_j \equiv S_j/N$, and $\tilde{j} \equiv 1 - (j-1)/N$. Define

$$Y_n \equiv \int_0^1 \prod_{j=1}^{n} \left(\gamma \left[X_j \frac{\tilde{j}}{t - \tilde{S}_{j-1}} - 1 \right] + 1 \right) d\gamma.$$

Polynomial in γ of degree at most n, with constant term 1.

Under the null, $(Y_j)_{j=1}^{N}$ is a non-negative closed martingale with expected value 1.

Ballot-comparison audits

Use cast vote records (CVRs): system's interpretation of each ballot.

Like checking an expense report.

b_i is ith ballot, c_i is cast-vote record for ith ballot.

A an assorter.

overstatement error for ith ballot is

$$\omega_i \equiv A(c_i) - A(b_i) \leq A(c_i) \leq u,$$

where u is an upper bound on the value A assigns to any ballot card or CVR.

$v \equiv 2\bar{A}^c - 1$, *reported assorter margin*.

$B(b_i, c) \equiv (1 - \omega_i/u)/(2 - v/u) > 0$, $i = 1, \ldots, N$.

B assigns non-negative numbers to ballots.

Reported outcome correct iff

$$\bar{B} > 1/2.$$

Stratified sampling

Cast ballots are partitioned into $S \geq 2$ *strata*.

Stratum s contains N_s cast ballots.

Let $\bar{A}_s^b$ denote the mean of the assorter applied to just the ballot cards in stratum s. Then

$$\bar{A}^b = \frac{1}{N} \sum_{s=1}^{S} N_s \bar{A}_s^b = \sum_{s=1}^{S} \frac{N_s}{N} \bar{A}_s^b.$$

Can reject the hypothesis $\bar{A}^b \leq 1/2$ if we can reject the hypothesis

$$\bigcap_{s \in S} \left\{ \frac{N_s}{N} \bar{A}_s^b \leq \beta_s \right\}$$

for all $(\beta_s)_{s=1}^S$ s.t. $\sum_{s=1}^S \beta_s \leq 1/2$.

Union-Intersection Test

Fisher's Combining Function

$\{P_s(\beta_s)\}_{s=1}^S$ are independent random variables.

If $\bigcap_{s\in S}\left\{\frac{N_s}{N}\bar{A}_s^b \le \beta_s\right\}$, distribution of

$$-2\sum_{s=1}^{S} \ln P_s(\beta_s)$$

is dominated by chi-square distribution with $2S$ degrees of freedom.

Low-dimensional optimization problem to maximize P-value over $(\beta_s)_{s=1}^S$.

Sample design

- individual ballots?
- clusters of ballots?
- stratify? (logistics, equipment capabilities, . . .)
- sampling probabilities?
- with replacement? without replacement? Bernoulli?
- fully sequential? batch-oriented?

Bayesian election audits

Limit the *upset probability*, the posterior probability that the reported outcome is wrong, given the sample, for a particular prior distribution on outcomes

Bayesian election audits

Limit the *upset probability*, the posterior probability that the reported outcome is wrong, given the sample, for a particular prior distribution on outcomes

Typically use Dirichlet-multinomial prior.

"Non-partisan" priors invariant under permutations of the candidate names.

A Bayesian Method for Auditing Elections

Ronald L. Rivest
Computer Science and Artificial Intelligence Lab,
MIT, Cambridge, MA 02139
rivest@mit.edu

Emily Shen
Computer Science and Artificial Intelligence Lab,
MIT, Cambridge, MA 02139
eshen@csail.mit.edu

Abstract

We propose an approach to post-election auditing based on Bayesian principles, and give experimental evidence for its efficiency and effectiveness. We call such an audit a "Bayes audit". It aims to control the probability of miscertification (certifying a wrong election outcome). The miscertification probability is computed using a Bayesian model based on information gathered by the audit so far.

A Bayes audit is a single-ballot audit method applicable to any voting system (e.g. plurality, approval, IRV, Borda, Schulze, etc.) as long as the number of ballot types is not too large. The method requires only the ability to randomly sample single ballots and the ability to compute the election outcome for a profile of ballots. A Bayes audit does not require the computation of a "margin of victory" in order to get started.

1 Introduction

This section provides a quick introduction to post-election audits and our notation. Section 2 then presents our proposed Bayes audit procedure. Section 3 gives the results of our initial experiments using this method on simulated and real election data. Section 4 considers some extensions and variations of the basic method, and Sections 5 and 6 discuss and summarize what we have learned about the Bayes audit. Appendix A provides some additional technical details on efficient implementation methods.

1.1 Post-election audits

Informally, the purpose of a post-election audit is to check that the reported election outcome is correct, by auditing enough randomly chosen ballots.

Absolute certainty isn't required of an audit (the only

Bayes/Frequentist duality

Risk of an audit for a set of cast votes and a reported outcome:

- probability of not correcting outcome, if reported outcome is wrong for that set of votes
- 0, if reported outcome is correct for that set of votes

Bayes/Frequentist duality

Risk of an audit for a set of cast votes and a reported outcome:

- probability of not correcting outcome, if reported outcome is wrong for that set of votes
- 0, if reported outcome is correct for that set of votes
- RLAs control *maximum* risk.
- Bayesian audits (Rivest & Shen) control *weighted average* of the risk. The prior sets the weights in the average.
- For 2-candidate plurality contest w/ no invalid votes, least-favorable prior has point mass $1/2$ at tie, remaining $1/2$ mass arbitrary over winning outcomes (Vora, 2018).

Wrinkles

- ~20% of U.S. voters don't vote on paper
- ballot-marking devices make the paper trail hackable: current suit in GA
- inadequate rules for chain of custody, ballot accounting, pollbook reconciliation, signature verification, ...
- transparent high-quality randomness
  - public ceremony of die rolls, published crypto-quality PRNG
- missing ballots; imperfect manifests
  - "Manifest Phantoms to Evil Zombies"
- ability to produce CVRs linked to ballots
- redacted CVRs

Open-source software

- auditTools
- ballotPollTools
- SUITE
- SHANGRLA
- Arlo

Evidence-Based Elections: 3 C's

- Voters *CREATE* complete, durable, verified audit trail.

Evidence-Based Elections: 3 C's

- Voters *CREATE* complete, durable, verified audit trail.
- LEO *CARES FOR* the audit trail adequately to ensure it remains complete and accurate.

Evidence-Based Elections: 3 C's

- Voters *CREATE* complete, durable, verified audit trail.
- LEO *CARES FOR* the audit trail adequately to ensure it remains complete and accurate.
- Verifiable audit *CHECKS* reported results against the paper

MIT News

Browse or Search

MIT researchers identify security vulnerabilities in voting app

Mobile voting application could allow hackers to alter individual votes and may pose privacy issues for users.

Abby Abazorius | MIT News Office
February 13, 2020

Press Inquiries

In recent years, there has been a growing interest in using internet and mobile technology to increase access to the voting process. At the same time, computer security experts caution that paper ballots are the only secure means of voting.

Now, MIT researchers are raising another concern: They say they have uncovered security vulnerabilities in a mobile voting application that was used during the 2018 midterm elections in West Virginia. Their security analysis of the application, called Voatz, pinpoints a number of weaknesses, including the opportunity for hackers to alter, stop, or expose how an individual user has voted. Additionally, the researchers found that Voatz's

PRESS MENTIONS

MIT researchers have identified security flaws in a mobile voting application that allowed some overseas and military citizens to vote remotely, reports Lydia Emmanouilid for PRI's *The World*. "When things a opaque — when you can't verify, whe you can't see what the code is doing says graduate student Michael Specter, "there is no way of vetting that it's doing the right thing."

"PR

3/30/2020
03:45 PM

HackerOne Drops Mobile Voting App Vendor Voatz

Bug bounty platform provider cited "Voatz's pattern of interactions with the research community" in its decision to halt the app vendor's vuln disclosure program on HackerOne.

Dark Reading Staff
Quick Hits

Mobile voting application vendor Voatz has been dismissed from HackerOne's bug bounty program platform, according to a report on CyberScoop.

Voatz — whose mobile voting app used in limited elections in a handful of states, including West Virginia and Colorado — has been under intense scrutiny over security concerns, and recently published studies by MIT and Trail of Bits uncovered significant security weaknesses in the app.

While security experts long have dismissed mobile voting as inherently risky, proponents of mobile-voting have maintained that the apps and process are more secure and private, for example, than the standard practice of sending PDF-based ballots via unencrypted email to military personnel overseas.

Voatz recently had updated its bug bounty policy on HackerOne to say that it could not "guarantee safe harbor" for researchers who discover flaws in its software under the program, CyberScoop said in its report.

FREE SPEECH FOR PEOPLE .ORG

April 20, 2020

The Honorable Ellen F. Rosenblum
Office of the Attorney General
Commerce Building
158 12th St. NE
Salem, OR 97301

Dear Attorney General Rosenblum,

We write to you to urge you to initiate an investigation into the voting system vendor Voatz for advancing potential false claims and deceptive marketing practices while promoting its mobile voting application in Oregon that may violate the Unlawful Trade Practices Act, Or. Rev. Stat. § 646.607; fraudulent misrepresentation; or any other violation of state law.[1]

Voatz is Boston-based startup company that is developing and aggressively marketing an internet-based voting system that enables voters to cast a ballot from application loaded on to their mobile phones. In 2019, Jackson and Umatilla counties contracted to have Voatz offer its internet voting system to voters eligible under the Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) for Oregon's 2020 general elections.

Voatz's campaign to promote its voting system in Oregon has included bogus claims of "military grade security,"[2] public statements asserting that votes cast on its platform could not be deleted or altered,[3] and published materials[4] and presentations[5] promising that Voatz's system was robustly vetted and secure.[6] Though many computer security


411412
511221
411413
521225
411418
561341
421224
421422
411221
421222
421225
421226