Evidence-Based Elections and Software Independence

Ronald L. Rivest

MIT

DEFCON Voting Village

August 8, 2025

Outline

- How we vote now: paper ballots
- **Evidence-based Elections**
- **Software Independence**
- Other Voting Systems:
  - Vote by Mail
  - Cryptographic Voting Schemes (E2E-V)
  - Hybrid
  - Remote (Internet) Voting ???

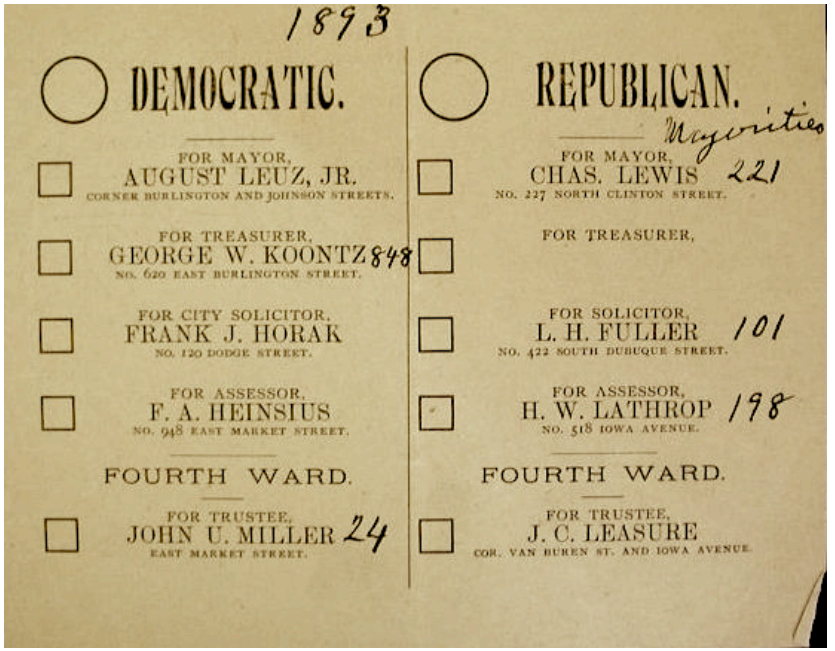
Nov. 2020 – Who Really Won?

Elections are fundamental to democracy!

How do we vote?

Paper Ballots, mostly

1893
"Australian"
Paper
Ballot



1893

DEMOCRATIC.

FOR MAYOR,
AUGUST LEUZ, JR.
CORNER BURLINGTON AND JOHNSON STREETS.

FOR TREASURER,
GEORGE W. KOONTZ 848
NO. 620 EAST BURLINGTON STREET.

FOR CITY SOLICITOR,
FRANK J. HORAK
NO. 120 DODGE STREET.

FOR ASSESSOR,
F. A. HEINSIUS
NO. 948 EAST MARKET STREET.

FOURTH WARD.

FOR TRUSTEE,
JOHN U. MILLER 24
EAST MARKET STREET.

REPUBLICAN.

Majorities

FOR MAYOR,
CHAS. LEWIS 221
NO. 227 NORTH CLINTON STREET.

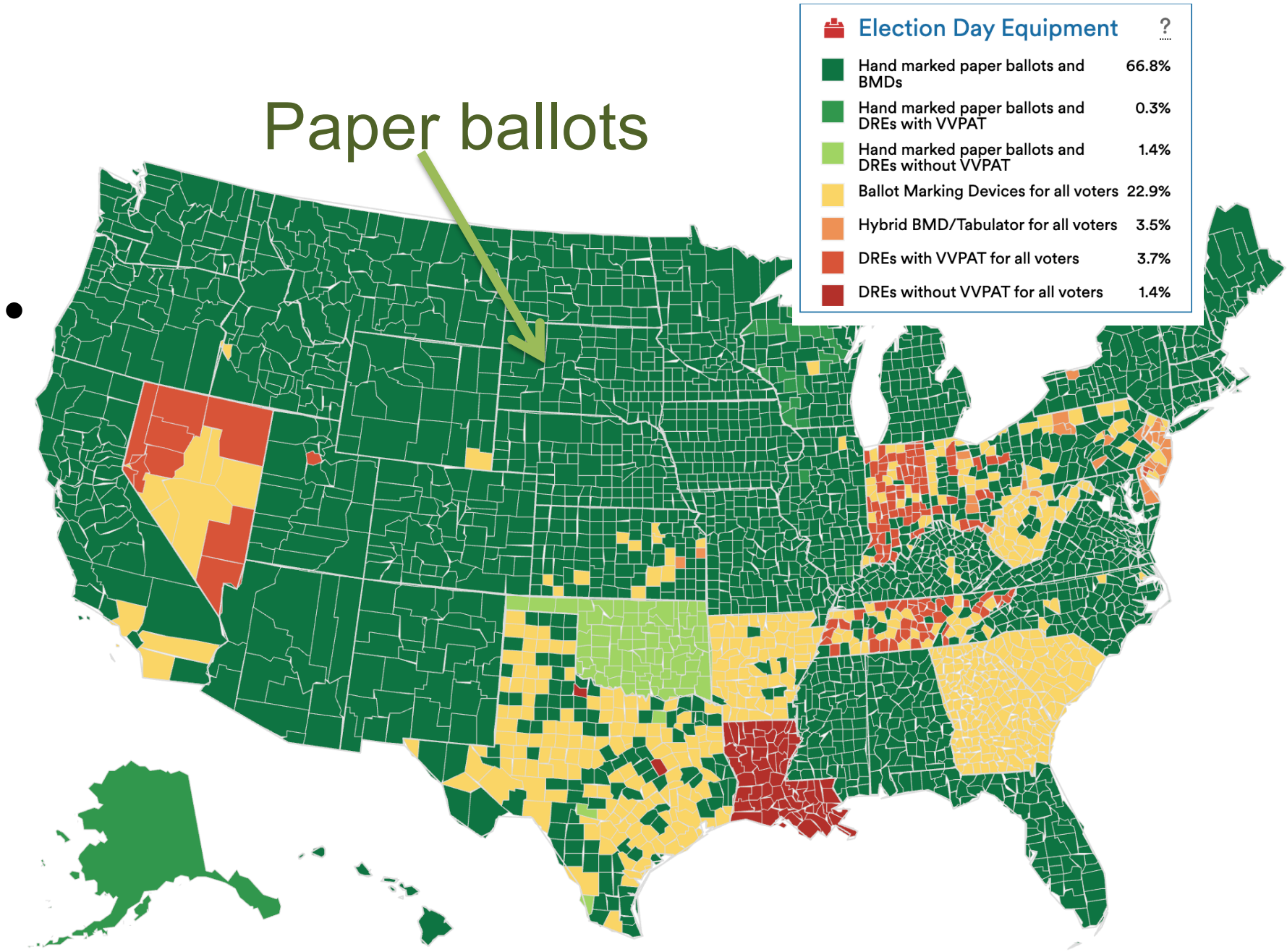
FOR TREASURER,

FOR SOLICITOR,
L. H. FULLER 101
NO. 422 SOUTH DUBUQUE STREET.

FOR ASSESSOR,
H. W. LATHROP 198
NO. 518 IOWA AVENUE.

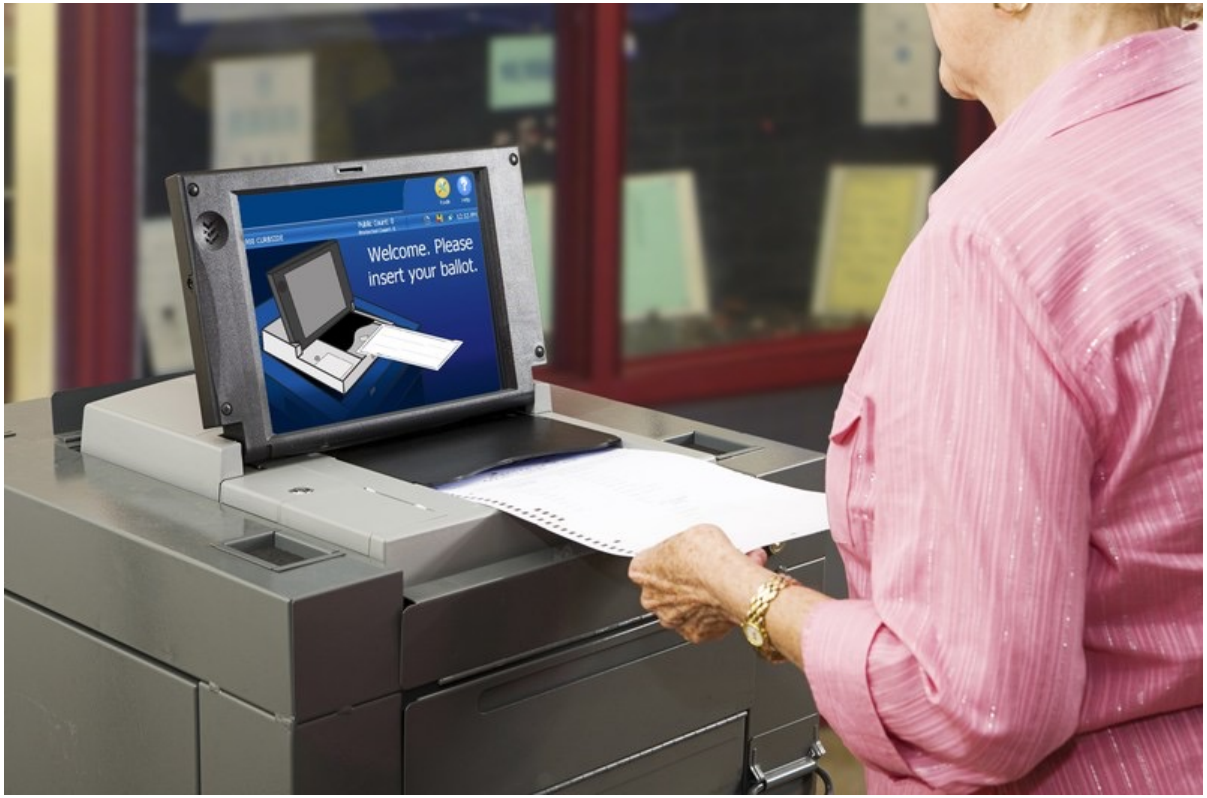
FOURTH WARD.

FOR TRUSTEE,
J. C. LEASURE
COR. VAN BUREN ST. AND IOWA AVENUE.



Verified Voting -- Projected for 2026

Optical scanners used for efficient tabulation, to give an “initial” outcome



Scanners may introduce errors due to:

- Differences in **interpretation** between machine interpretation, and hand interpretation based on “voter intent” rules.
- **Stray marks** (e.g. caused by folds)
- **Configuration and programming errors**
- Hacking (**adversarial attack**)

How *should* we vote?

Voting is hard and complicated

- Not like online banking – votes are *anonymous*
- No one, and no piece of software, is trusted
- Voters must authenticate themselves
- Election must produce *evidence* outcome is correct
- Disabled voters, rank-choice voting, dispute handling, voters shouldn't have to supply equipment, voting must be "fire-and-forget"…

Security Requirements

Security Requirements

- Only eligible voters may vote
- Each eligible voter votes at most once.
- Each cast vote is **secret**,
  even if voter wishes otherwise!
  -- No vote-selling!
  -- No receipt showing how you voted!
- Final outcome is **verifiably correct**.
- No ``trusted parties'' – **all are suspect**!
  Vendors, voters, election officials, candidates,
  spouses, other nation-states, …

Evidence-Based Elections

An election system should not only

accurately figure out who won,

but should also

provide convincing evidence
that the winner really won.

(Stark & Wagner 2012)

Cast ballots are best evidence

- The best evidence as to who won an election is the ***collection of voter-verified cast ballots:***
  - Each ballot verified as accurate by the voter who cast it. This is the ``**ground truth''.**
  - Authenticity of collection assured by verifiable **chain of custo**dy

Software Independence

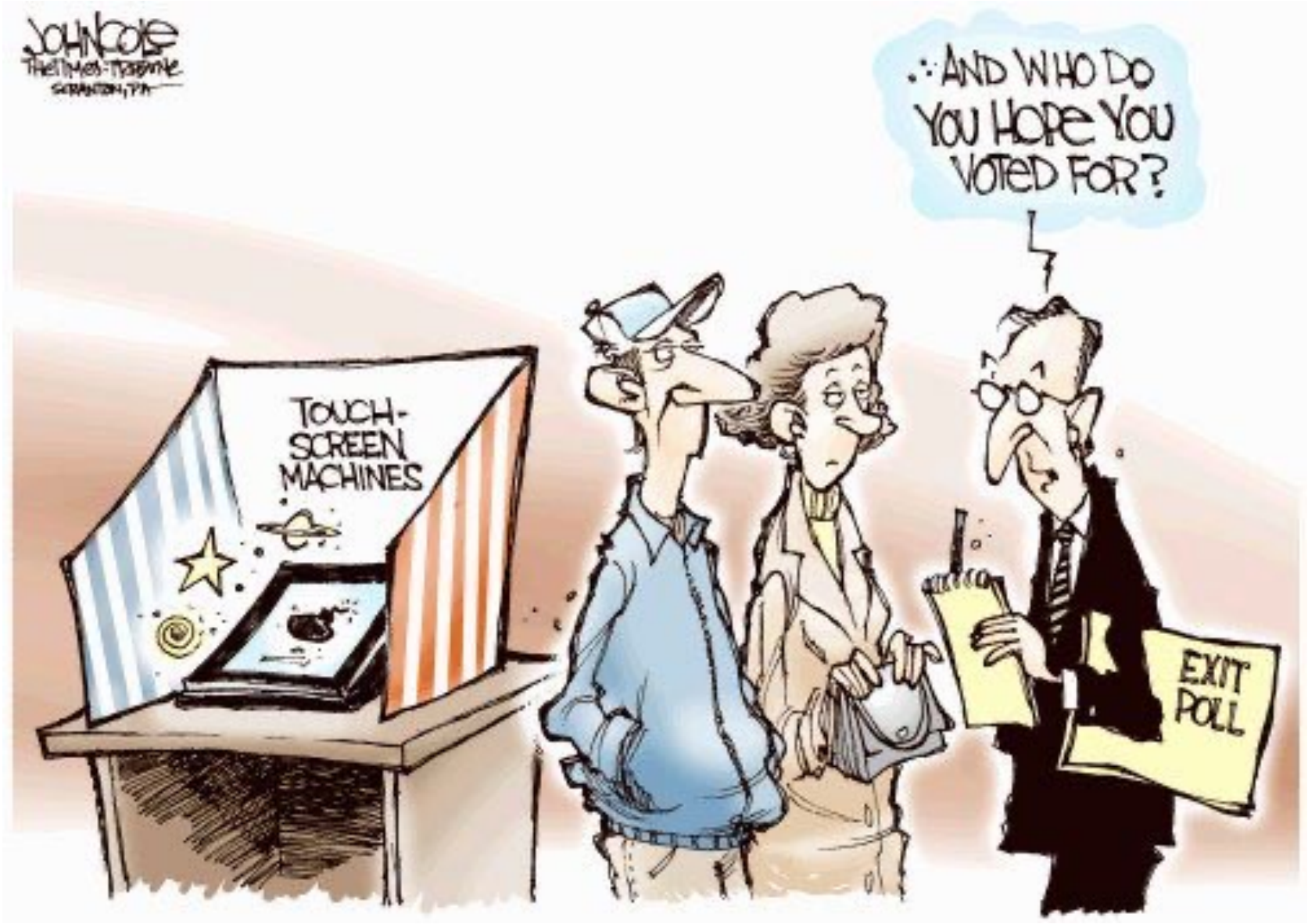
(Rivest & Wack, 2006)

Software Independence

- Software is *not* to be trusted! It can be self-modifying and self-erasing! We don't have any good methods for determining if a voting system is running the right software!
- A voting system is *software independent* if **an undetected error in the software can <u>not</u> cause an undetectable change in the election outcome**.
- ***Strongly*** *software-independent* if it is possible to correct any such outcome error

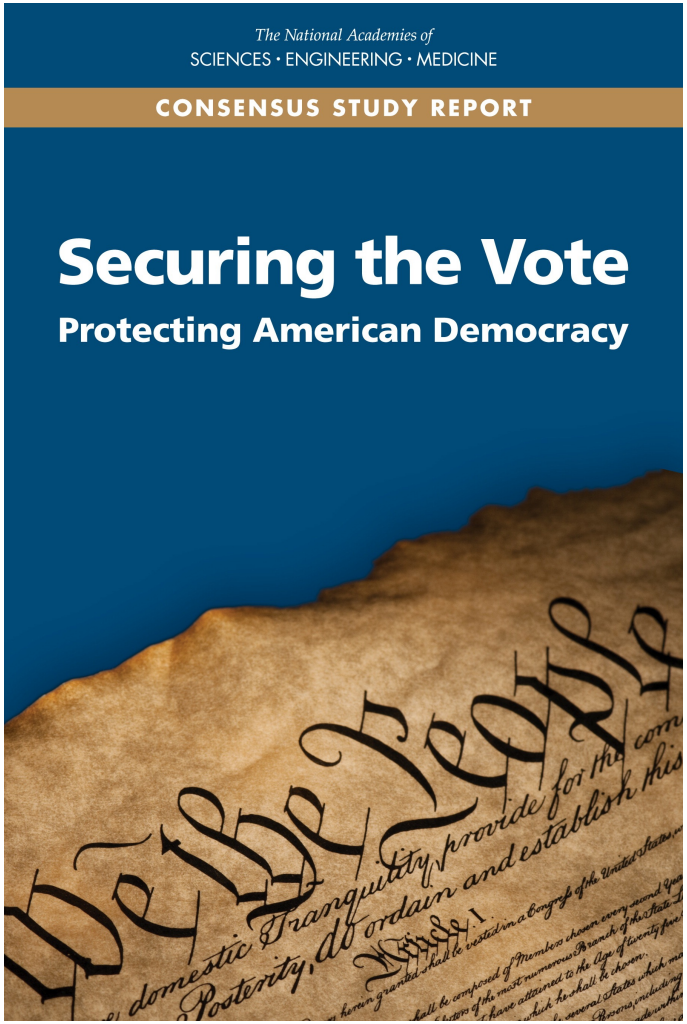
Software Independence (cont.)

- Example: Paper ballots (with hand recount)
- I'd be happy if all voting system software were made public!
- Stealing the voting system software means little - the **cast ballots** are the evidence, not the **software**!
- An adversary, foreign country, or even one of the candidates could provide the voting system software! (As long as you audit!)



And Who Do You Hope You Voted For?

NASEM Report (9/6/18)



National Academies issued report on

``**Securing the Vote**"

www.nap.edu/futureofvoting

(159 pages; free pdf)

41 recommendations

NASEM recommendation 4.12

Use *voter verifiable paper ballots* everywhere by 2020

NASEM recommendations 5.7—5.9

Audit election outcomes!

NASEM recommendations 5.7—5.9

Audit election outcomes!

A ***risk-limiting audit (RLA)*** *uses manual interpretation of randomly chosen cast paper ballots to verify with high probability the reported election outcome (or correct it, if wrong).*

The Post's View • Opinion

A simple step every state could take to safeguard elections

Voters at a polling place in Columbus, Ohio, in October 2018. (John Minchillo/AP)

By **Editorial Board**

Oct. 21, 2019 at 7:31 p.m. EDT

Election Process (paper ballots)

- Print ballots; setup
- Mark Choices; **Voter Verifies Vote**; Cast Vote!
- Optical scanners give initial ("reported") outcome
- **Statistical audit of cast paper ballots** by hand to confirm/disprove reported outcome

Auditing of Paper Ballots

Audits are about:

- Sampling cast paper ballots at random
- Figuring out what the **evidence** (sampled ballots) says about the reported election results.
  - *Risk-Limiting audits (or other methods)*
- *Efficiency:* An RLA often looks at 0.1%--10% of the cast ballots $(3/margin)$. A 200% speedup, sometimes, compared to a full hand recount!

Three auditing paradigms

- **Ballot-comparison audits**:
  Compares each paper ballot with its electronic record (“cast vote records’’)
- **Ballot-polling audits**:
  Uses cast paper ballots only.
  Like ``exit poll’’ of ballots…
  Less efficient than ballot-comparison audit
- **Batch-comparison audits:**
  Like ballot-polling audits, but looks at ballots a batch at a time. Least efficient.
- Image-based ``audits’’ 

What question is RLA asking?

- What is current ``risk''?

  Probability that

  if reported winner is incorrect,

  audit would accept it

  if audit stopped now.

- Stop sampling ballots when risk is below limit.
- RLA does **not** prove correctness of tally (ref NPV!), ask about voter eligibility or authentication; it assumes chain of custody.

Who is audit for?

All stakeholders:

- **The winner –** to provide a mandate
- **Losing candidates** – to convince them that "they lost fair and square"
- **Election officials –** to help them provide accurate and efficiently-verified results
- **The public** – to ease doubts about a "rigged election"

Auditing other outcome rules

Social choice functions

- Not all elections are *plurality*
- Some elections are *ranked-choice:*
  ballot gives voter's preferences:
  $$A > C > D > B$$
- A ``social choice function'' maps collections of ballots to outcomes.
- Example: IRV (Instant Runoff Voting)
- Methods exist for auditing **all** other voting methods (e.g. Bayesian audits)

Remarks

- Other auditing methods (e.g. Bayesian) handle all cases, e.g.
  - Hybrid audits (where only some ballots have cast-vote records)
  - Other complex voting schemes
- For more details see https://arxiv.org/abs/1801.00528

Mail-in Voting

Same as in-person hand-marked paper ballots, except that ballots are cast via US mail.

End-to-end Verifiable Voting

(E2E-V)

E2E-V

- Heavily cryptographic; complex
- Evidence is electronic; encrypted votes on public bulletin board
- Provides "end-to-end" integrity; votes are
  - "**cast as intended**" (*verified by voter)*
  - "**collected as cast**" (*verified by voter or proxy)*
  - "**counted as collected**" (*verified by anyone)*
- Has been used in real elections (ElectionGuard Microsoft): WI, CA, ID, UT, MD)

Hybrid Voting (paper + E2E-V)

Best of both worlds?
paper + electronic E2E-V

- Some hybrid systems have *both:*

  a paper ballot **and**

  an electronic E2E-V subsystem.

- Can RLA-audit paper ballots,

  and

  can audit electronic records on PBB as usual for E2E-V system.

Internet voting 

(Mobile phone voting) 

NASEM recommendation 5.11

No *Internet voting*!

- **PRESS RELEASE (COMMON CAUSE)**
- **New Berkeley Report Prompts Call for Deep-Pocketed App Promoter to Scrap Vulnerable Online Voting Plans**
- Published: Dec 14, 2022
- Today, the University of California Berkeley Center For Security in Politics issued a statement reporting on the conclusions of a Working Group convened with funding from Tusk Philanthropies to develop standards that would ensure internet voting can be secure and private. The Working Group concluded that it could not issue such standards, stating "*the current cybersecurity environment and state of technology make it infeasible for the Working Group to draft responsible standards to support the use of internet ballot return in U.S. public elections at this time*."

Conclusions

- We can make elections much more secure with post-election audits and maybe cryptography.
- End-to-end verifiable voting methods look viable, and may be desirable long-term.
- Hybrid methods with paper+E2E look good!
- We are not yet ready for ``internet voting,'' (aka "mobile voting"); it is at best *years* away!
- **Evidence-based elections**, **SI** are way to go!

The End

Thanks for your attention!

(and thanks to Verified Voting!)

Questions?