Election Security

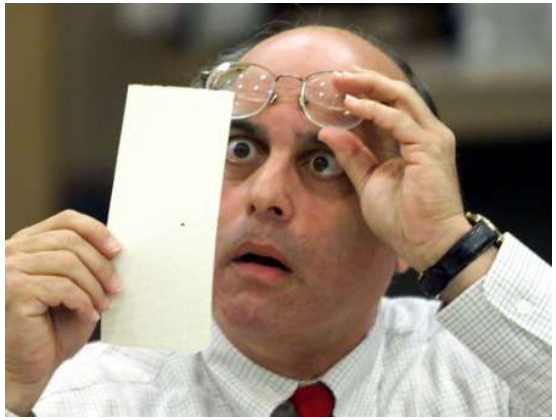
Ronald L. Rivest
MIT

2019 D.C. Circuit Judicial Conference
June 26, 2019

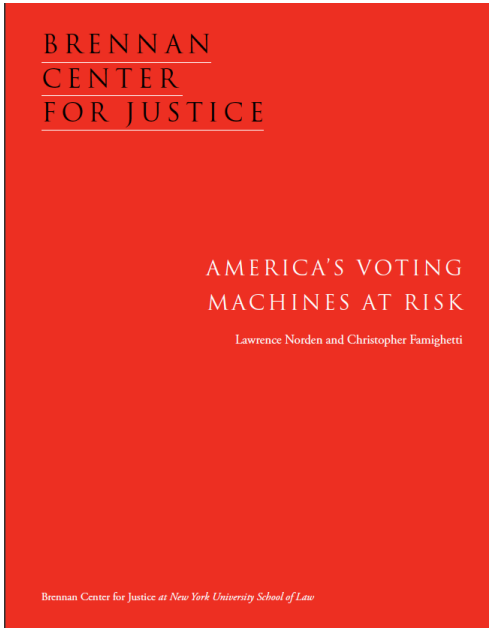
Outline

- Security Requirements
  - Evidence-based Elections
  - Software Independence
- Auditing of Paper Ballots
- Remote (Internet) Voting ???

Have we made progress since 2000?



Hanging chads
(2000)



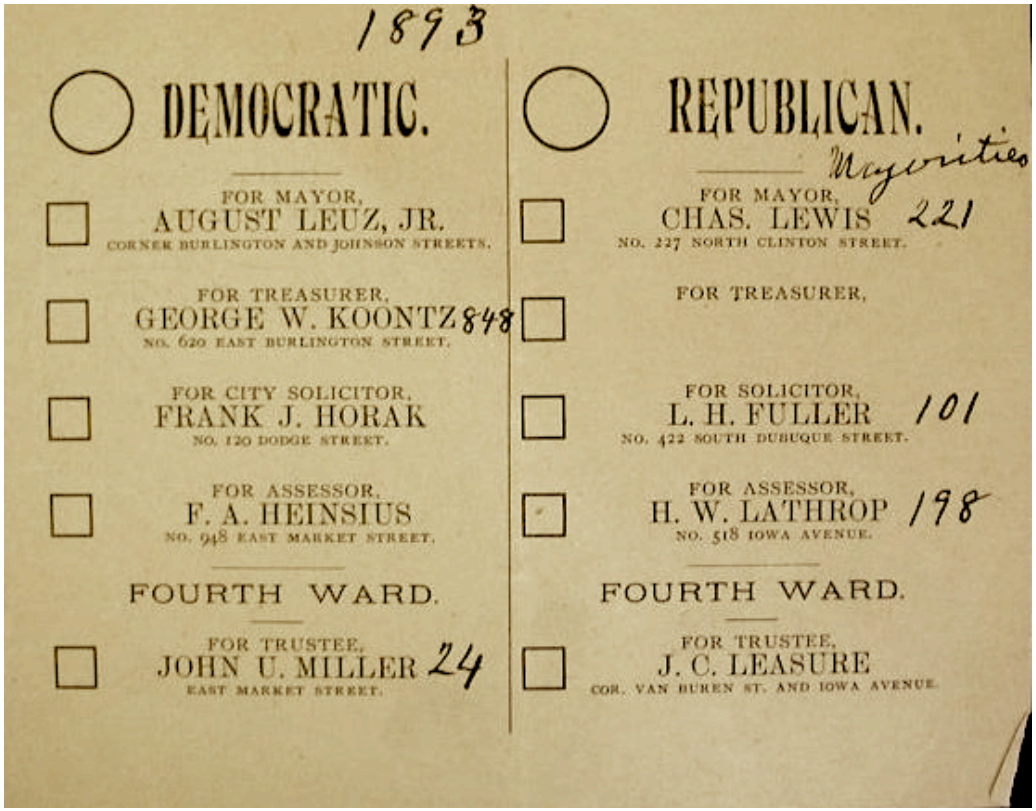
Voting Machines at Risk (2015)

Nov. 2016 – Who Really Won?

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.

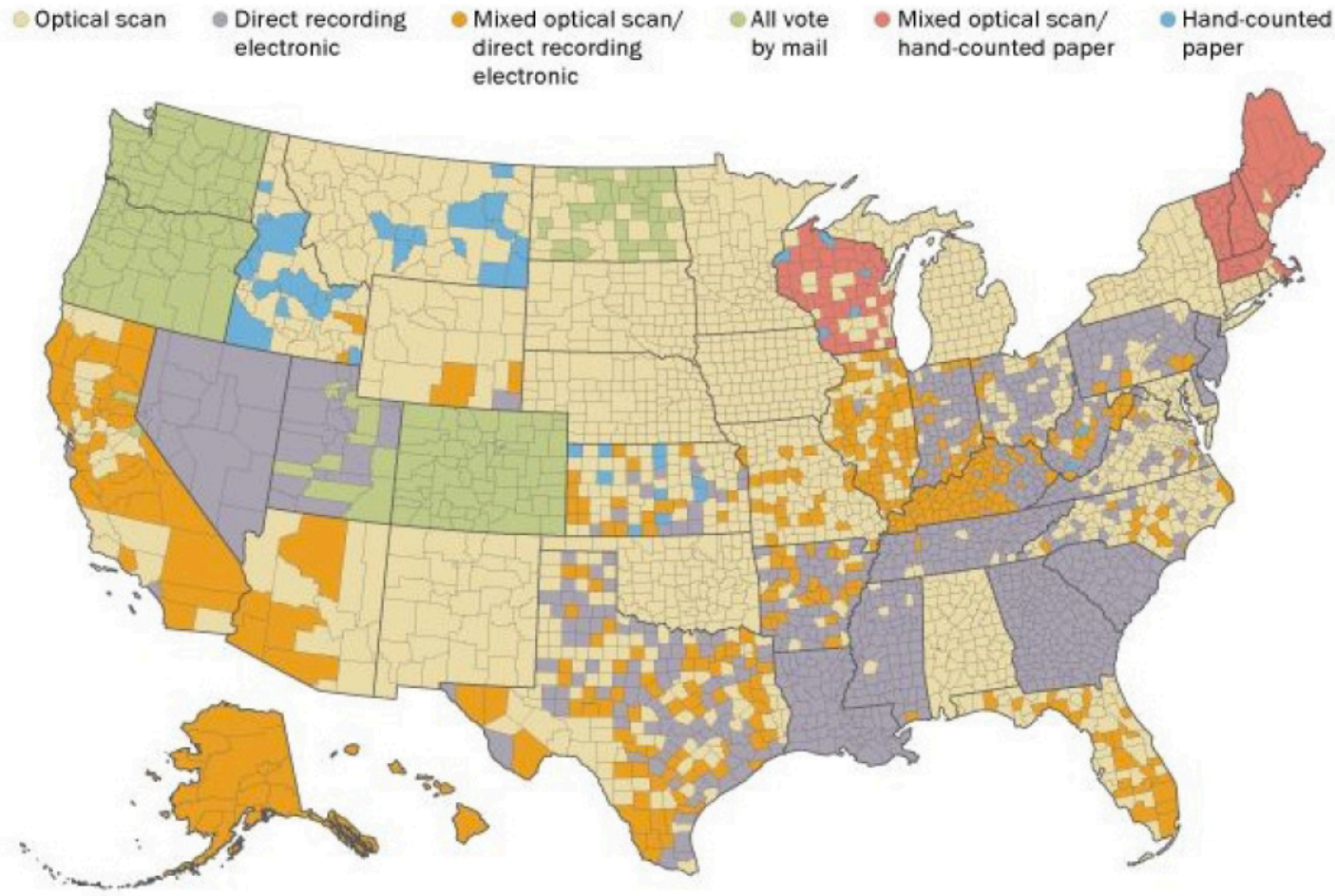
FOR TREASURER,

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.



About 80% of voters use paper ballots

Optical scanners are used for efficient tabulation


DOMINION
VOTING
Security Key
OPEN
System Ready
BALLOTS CAST: 72
Cast
Return

(Concern:) Scanners may introduce systematic errors

Causes of scanner errors

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

How *should* we vote?

Security Requirements

Security Requirements

- Only eligible voters may vote, and
  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,

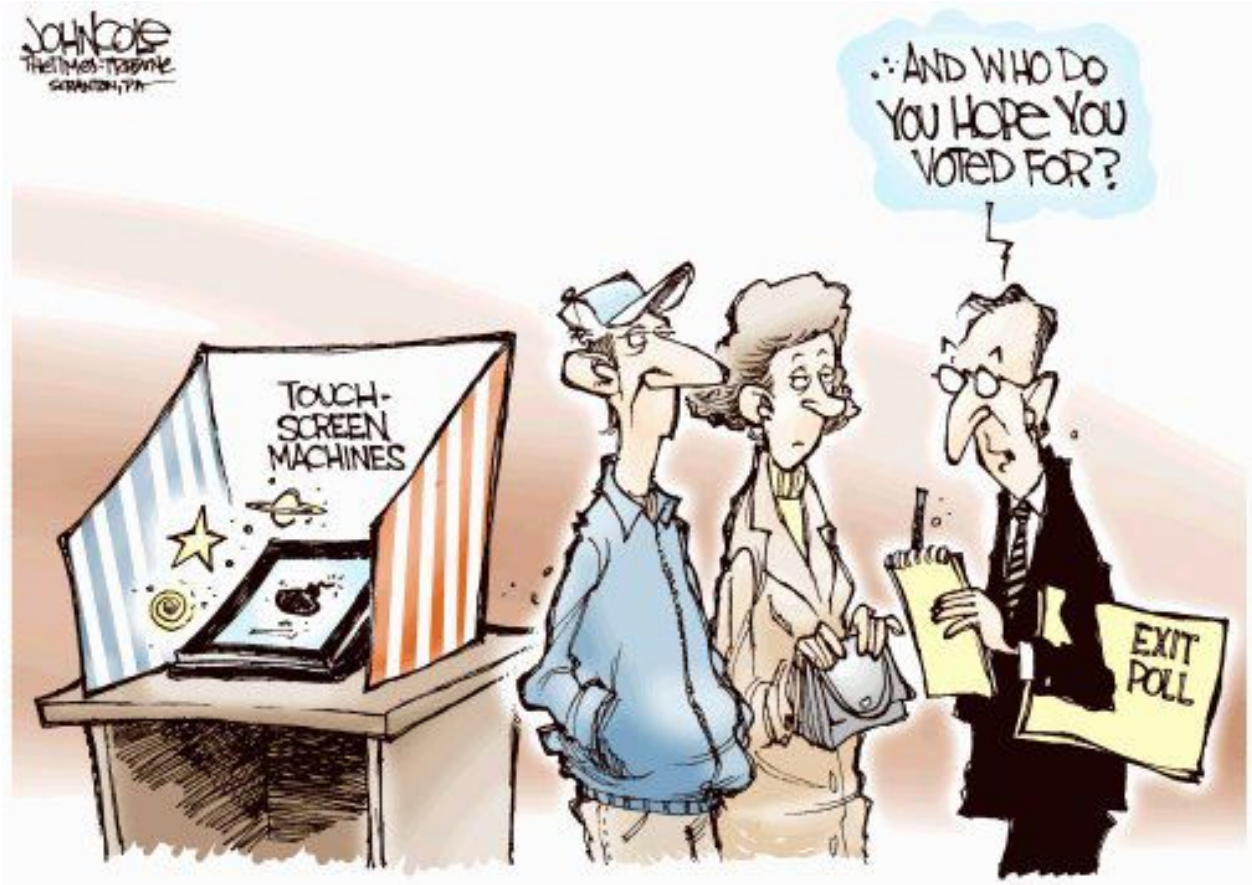
but should also

provide convincing evidence
that the winner really won.

(Stark & Wagner 2012)

Software Independence

(Rivest & Wack, 2006)

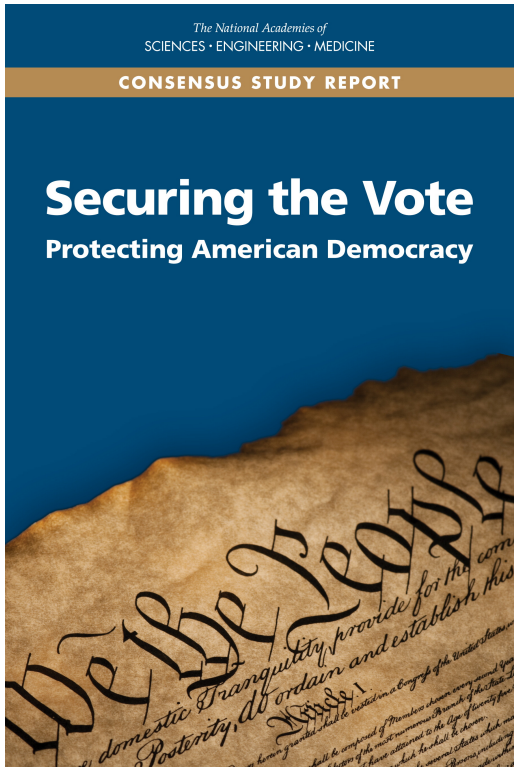


And Who Do You Hope You Voted For?

Software Independence

- Software is *not* to be trusted!
- A voting system is *software independent* if
  an undetected error in the software can not cause an undetectable change in the election outcome.
- *Strongly software-independent* if it is possible to correct any such outcome error
- Example: Paper ballots (with hand recount)

NASEM Report (9/6/18)



National Academies issued report on

"**Securing the Vote**"

www.nap.edu/futureofvoting

(159 pages; free pdf)

41 recommendations

Recommendation 4.12

Use *voter verifiable paper ballots* everywhere by 2020

Recommendations 5.7—5.9

Audit election outcomes!

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).*

Election Process (paper ballots)

- Print ballots; setup
- Mark Choices; **Verify Vote**; Cast Vote!
- Optical scanners give initial ("reported") outcome
- **Statistical audit of cast paper ballots**
  by hand to confirm/disprove reported outcome
  - "Brush your teeth; eat your spinach;
    audit your elections!" -- Poorvi Vora

Auditing of Paper Ballots

Audits

- Sample cast paper ballots at random
- Figuring out what the sampled ballots tell you about the reported election results
  - *Risk-Limiting audits*

Who is audit for?

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

What a RLA does **not** do

- A RLA does not address:
  - **correctness of the *tally* (as opposed to the outcome)**
  - **voter eligibility**
  - **voter authentication**
  - **usability**
  - **privacy**
  - **chain of custody of paper ballots**

Audit Rochester Hills MI (12/3/2018)

- Reported results for Proposition:

  22,999 **Yes**
  12,343 **No**
  1,324 **Other**

- Sample results for Proposition:

  50 **Yes**
  26 **No**
  0 **Other**

- *So… ???*

Risk-Limiting Audit

- **RLA Question**:
  What is current ``risk''? (Probability that if reported winner is incorrect, audit would nonetheless accept it if audit stopped now.)

Results

- **RLA results:**

  Risk measured at 2.1 %

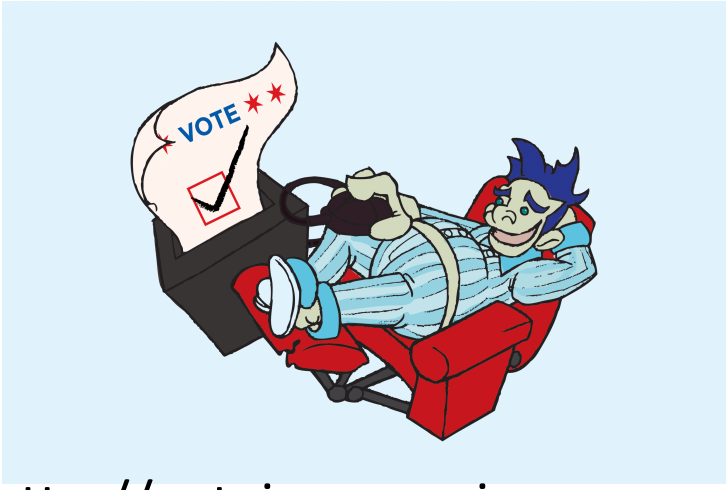
  (Kellie Ottoboni using SUITE tool)

- **Reported outcome confirmed (accepted by audit) after only 76 ballots sampled!**

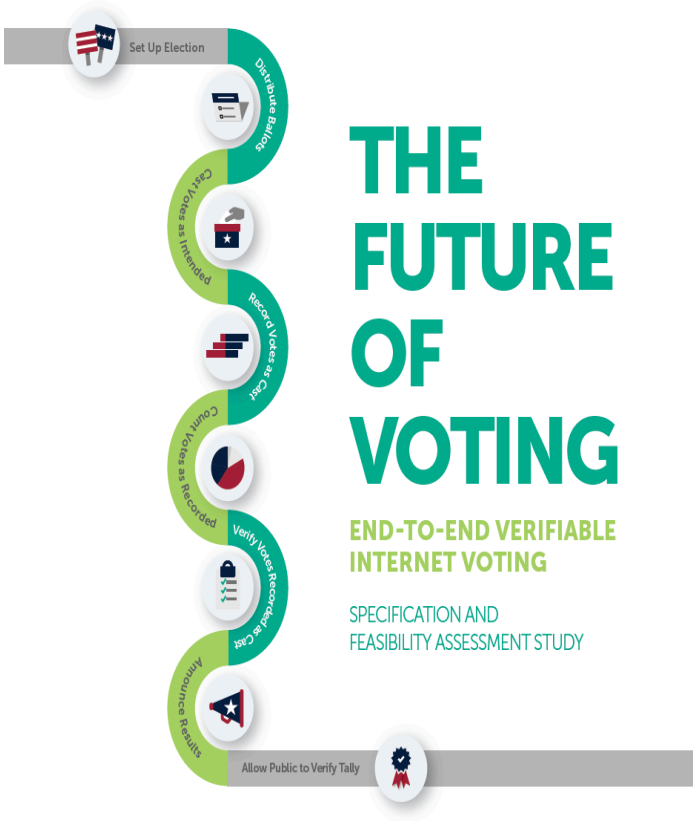
Recommendation 5.11

No *Internet voting*!

When can I vote on the Internet? (or on my phone?)



http://voteinyourpajamas.org/



- U.S. Vote Foundation 2015 Report on Internet Voting:
  - **Internet voting requires solutions to many as-yet-unsolved problems:**
    - Malware
    - DDOS attacks
    - Authentication
    - MITM attacks
    - Zero-day attacks on servers
    - Coercion & vote-selling
    - …

Conclusions

- We can make elections much more secure with post-election risk-limiting audits.
- We’re not yet ready for ``internet voting,’’ and may not be for 20 years…

The End

Thanks for your attention!

(and thanks to NSF CSOI and to Verified Voting!)