Voting in the Age of COVID-19

Barbara Simons

Indiana

- A crazy quilt of polling place voting technologies
  - More than ½ of state uses paperless systems
    - Insecure and old technology
  - ~ ¼ uses hand marked paper ballots (ideal)
    - Monroe County
    - https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020/state/18
- Mail-in ballots (need excuse to vote absentee)
  - Early processing - results unlikely to be significantly delayed
  - Will **NOT** accept mail-in ballots after Election Day, independent of postmark
- Internet voting
  - Allows email and fax return for overseas military – insecure/no secret ballot

How did we get here?

Computers introduced into elections without analysis of risks

- Florida 2000/2002 – hanging, pregnant, etc. chads
  - Paper bad; paperless good
- Help America Vote Act (2002) allocated ~$4B for new machines
  - Vendor promises
    - Secure
    - Just touch button at end of election
    - Federally certified
    - Deadline for spending money
    - Gold rush mentality – latest and greatest
  - Some orgs representing voters with disabilities pushed paperless systems

Early use of Computers in voting

- Initially many paperless Direct Recording Electronic (DRE) (still in IN)
  - Typically touch screen: displays, records, and tabulates votes
  - Calibration an issue: jumping votes
  - Badly engineered – cannot be recounted
  - Failures or insufficient numbers can create long lines
- In response to calls for “paper trails” – retrofitted DREs (still in IN)
  - Voter Verified Paper Audit Trails as hard copy backup to computer
  - Continuous roll thermal printed – like gas receipts – easily fade – hard to count
  - Often small font – hard to read – typically under transparent plastic
  - MIT study: few people checked – didn’t know was intended to validate vote

Testing and Certification

- Voluntary federal guidelines – initially minimal security and accessibility testing – computer security experts not involved
  - Recent draft guidelines far better, but not yet implemented
- State testing led by computer security experts
  - California Top-to-Bottom-Review (TTBR) (2006)
    - Many Univ. of California scientists involved
    - Tested all aspects of 3 systems, including security & accessibility
    - Everything bad
  - Ohio EVEREST (2007)
    - Confirmed all problems discovered in TTBR and found additional ones
- Other studies confirmed security problems

2020

In-person voting

- Poll workers tend to be elderly
  - C-19 risk
  - Need to involve many more younger people – please consider volunteering
- Need PPEs and sanitizers + sufficiently large space for safe distancing
  - Some sports arenas being made available
- If voters required to vote on machines, insufficient number or break downs can disenfranchise voters
  - Risk for any voting machines, both old DREs and new Ballot Marking Devices

Mail-in ballots

Preprocessing

- Sort envelopes by “ballot style” (municipality or district)
  - Based on information on envelope, look up voter’s information in voter-registration database (VRD)
  - Do signature comparison using database
    - If matches, accept envelope and mark voter in VRD as having voted
    - If missing or doesn’t match, could inform voter and provide option to fix problem
      - Not all states provide this option
      - Not possible if processing started very late, i.e. Nov 2 or 3
  - Remove identifying info from envelope or discard outer envelope to protect secret ballot
  - Some states allow early ballot tabulations, but results must be confidential until ED
- Early preprocessing can speed up results
  - Not allowed in some states

States that encourage mail-in ballots

- Already primarily vote-by-mail: should run fairly smoothly
  - OR, UT, CO, HI, WA
- Vote-by-mail request forms sent to all voters + in-person voting
  - Some planning early pre-processing, while others start on Nov 2 or 3
    - Lack of early pre-processing could cause major delay in tabulations: IO, MI, WI
- VT mailing ballot to every voter, but no processing until Nov. 2
  - Determination of results likely to be delayed
- Some states allow late ballot arrival if postmarked by Election Day
  - California <= 17 days after Election Day
  - Others require ballots to be received by Election Day

Potential issues with vote-by-mail

- Significant increase in 2020
  - Could be problem for states that normally have little remote voting
    - Delays in Pennsylvania caused by lawsuits (e.g. GOP June lawsuit against drop boxes)
      - Sept 17 PA Supreme Court: ballots postmarked by ED <= 3 days later +dropboxes ok
      - Sept 22 PA GOP announced will appeal to US Supreme Court
- Blank ballots not received/voted ballots not returned in timely fashion
  - Problems with postal service
    - Post office doesn't postmark prepaid mail, but can provide evidence of when mailed
  - Other potential problems: states delayed in mailing because of court action, insufficient number of workers because of C-19, supply chain issues, etc.

On Election Day

- Open envelope with ballot
- Prepare ballot for scanning
  - If ballot can't be read by tabulating scanner, remake (copy by hand)
    - Obvious issues
  - Flatten ballot and put in batch for high-speed scanning + counting
- Scan ballot
- *Vote-by-mail meltdowns in 2020?* by Andrew Appel
- https://freedom-to-tinker.com/2020/09/20/vote-by-mail-meltdowns-in-2020/

Scanners count almost all paper ballots

- Both in-person and vote-by-mail

But…

- Scanners are computers - subjected to all the vulnerabilities of computers, including software bugs and hacks

Myths about election security

- Myth1: Machines never connected to internet, so can't be hacked
  - Other computers program voting machines and scanners with info about election: candidate names, location on ballot, etc.
    - Transferred to machines or scanners via portable memory device
  - These computers typically are connected at some time and could become infected - then infect voting machine or scanner
    - Stuxnet Virus that brought down Iranian centrifuges
- Myth 2: So many different types of systems, impossible to rig an election
  - Electoral college – don't need to attack everything
  - Can impact national election by focusing on small number of swing precincts in swing states

The solution

- Voter marked paper ballots – ideally hand marked
- Strong Chain of Custody
- Statistically sound manual post election ballots audits called Risk Limiting Audits

Voter Marked Paper Ballot Systems

- Voter manually marks ballot
- Typically counted by scanners
  - Can be at polls or in a central location
- If long lines or polling place scanner is down, voters can mark paper ballots and deposit in ballot box for later scanning

New Ballot Marking Devices (BMDs)

- BMDs > $$ than hand marked paper ballots
- Most print only voter's selections on paper ballot
  - New LA BMD lists every race, with "No Selection" for unvoted races
- Parts of some states & GA: all polling place voters must use BMDs
  - "Accessible" for voters with disabilities
- Need to verify ballots
  - Early results suggest not done in sufficiently large numbers
    - How to get voters to check their ballots?

Some bad BMD designs

- ES&S ExpressVote “permission to cheat” by giving voters option of not viewing voted ballot (used in Elkhart, Porter, Marion, & Dearborn Counties)
  - Cheating machine could print different selections if voter doesn’t look
- Dominion ImageCast Evolution can allow voted ballot to pass under printer
  - Printer could add votes or create overvotes

Post-election ballot audits

- Preliminary results reported before audits
- Audit must be completed before certification of results
- Manual count
- Random selection of ballots
- Risk Limiting Audits
  - Recommended by:
    - Presidential Commission on Election Administration
    - National Academies of Science, Engineering, and Medicine
    - The Senate Intelligence Committee
  - Developed by UCB Statistics Prof. Philip Stark

Risk Limiting Audits

- A check on the computers that tabulate votes to determine if reported outcome correct
  - Manually examines a sample of ballots
- Guaranteed large, pre-specified chance of correcting wrong reported outcome
  - An outcome is wrong if it disagrees with the outcome that a full hand count would obtain.
  - The largest chance that a wrong outcome will not be corrected by the audit is the risk limit of that audit.
    - E.g. if risk limit is 10%, then if the outcome is wrong, there is at least a 90% chance that the audit will lead to a full hand count that corrects it

RLAs: still a lot of uncertainty

- State laws
  - Colorado, starting with 2018 midterm
  - Rhode Island & Georgia first time Nov 2020
- Michigan and Pennsylvania likely, but not definite
  - SoSs want them, but don't have authority to order them
  - Both had conducted pilot RLAs earlier
  - Even if don't manage to conduct RLAs, will likely conduct decent audits
- VA has law, but audit unlikely to be conducted before recount deadline
- AZ – hope to have RLA in every county
- Most likely tipping point states have reasonable audit laws (if not RLAs)
  - FL bad recount laws (limited and only rescans): legacy of FL 2000

What we should NOT do

Internet voting, including cell phone and blockchain

Wawa
Capital One
Marriott
Facebook
Google+
Ashley Madison
Office of Personnel Management (OPM)
Pentagon email
Jeep
Sony
IRS
Target
Anthem Health Insurance
White House
JP Morgan
Kmart
State Department
Dairy Queen
AOL
Google
Symantec
Yahoo!
Northrop-Grumman
Juniper Networks
Charles Schwab
FBI
Adobe
USPS
Governments of: Germany, France, Iran, UK, Canada, Australia, …, and the UN

Stating the Obvious

How can underfunded, understaffed, under resourced local elections officials with little to no:

computing proficiency

computer security expertise

Protect their servers in an internet based election from well financed adversaries:

Foreign countries

Political operatives

Rogue hackers

Possible nation-state attacks

- “DHS assessed that the [Russian] searches, done alphabetically, probably included all 50 states, and consisted of research on 'general election-related web pages, voterID information, election system software, and election service companies”.
  - Senate Intelligence Committee report (Aug 2018) on Russian interference in the 2016 election
- No evidence exists of votes having been changed in 2016
  - No way to know, since can’t check paperless systems and most states with paper ballots didn’t conduct adequate post-election audits
- Many countries capable of attacks: e.g. Russia, China, N. Korea, Iran

What is internet Voting?

- Returning a voted ballot over the internet
- Via web, an email attachment, or fax
  - Email voting perhaps even more dangerous than web based
    - Modification en route, lost ballots, no secret ballot, ballot box stuffing with counterfeit ballots, etc.
  - Some confusion re if email is internet voting
- Personal computer, smart phone, smart tablet, etc.
- Ongoing research using crypto, but prominent cryptographers oppose implementation for foreseeable future

Internet Voting Used in U.S.

- ~30 states: military and overseas voters can return voted ballots over the internet
  - Some “pilot” real elections conducted in 2020 not limited to military
    - Claim were secure – impossible to know (but who would hack a pilot?)
- MOVE Act (2009) – eliminates delay of mailing blank ballot
  - Online posting of blank ballots at least 45 days before election
  - Voter downloads, prints, marks, and returns via postal mail
  - Expedited postal mail return of paper voted ballot for military
- A solution in search of a problem
  - Major BC study showed internet voting does NOT increase participation in general or by young people in particular
  - Similar results from Estonia and Switzerland

Regulations for Internet Voting

- None!! No: independent standards, independent testing, government oversight, legal accountability, ability to recount
- NIST asked to develop standards
  - Produced reports, but no standards
    - “Technology that is widely deployed today is not able to mitigate many of the threats to casting ballots via the web.”
    - “Malware on voters' personal computers poses a serious threat that could compromise the secrecy or integrity of voters' ballots.”

Vulnerabilities

- Authentication
- Malware on voters' devices can change votes without voters' knowledge or discards votes altogether (Jeff Bezos' iphone)
  - What you see on the screen many not be what is sent out over the internet
- Denial of Service attacks can prevent real ballots from reaching election officials
- Penetration attacks on vote servers can change votes
- Cannot be audited, since can't be certain that votes accurately recorded
- Secret ballot at risk
- Vote buying/selling; voter coercion

“Mobile” voting

- Use smart phones, which communicate over the internet
- Because “internet voting” has been given a bad name, call the systems “mobile” voting
- Two major vendors: Democracy Live and Voatz
- Both have been shown to have security vulnerabilities by independent cybersecurity experts
- Neither federally tested or certified
- No testing in mock elections where anyone allowed to hack
  - DC 2010
- Both have been deployed in “pilot” REAL elections
  - Tusk Philanthropies funding pilots

“Mobile” voting (con’t)

- Democracy Live’s system called OmniBallot
  - Website states that is not an online voting system
  - Ballot sent from smart phone over the internet
  - Claims that recount can be conducted by downloading and printed out paper copy
  - No way to know if print-out accurately represents voter’s choices
- Voatz “blockchain” voting
  - Two independent security reports uncovered serious vulnerabilities

Blockchain Voting:
The National Academies of Science (2018)

"In the particular case of Internet voting, blockchain methods do not redress the security issues associated with Internet voting."

Info about types of voting systems used throughout the country available at https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020