

CVRs and Ballot Images aid Security, Democracy

Election Verification Network Conference

Neal McBurnett, Election Integrity Consultant

2023-03-17

Neal McBurnett

- Consultant
- Software developer at Bell Labs etc.
- Working on election audits and integrity since 2003
- Poll worker
- Pioneered RLAs in Colorado with my own code in 2010, Boulder County
- On teams that wrote the software for Colorado's current state-wide audit
- Volunteer Voting Board member
- LWV Colorado Election Security position, 2022
- Audited Scantegrity II E2E verifiable Takoma Park MD election in 2011
- Speaking for myself

Priorities for the use of Cast Vote Records and Ballot Images

Wide agreement:

- Committing to data to be audited before random selection, without revealing it
- Publishing actual data so the public can validate, follow along during audit

My position:

- Obfuscating data reduces public trust

Huge opportunity that needs robust discussion:

- Leveraging data for the public good

Take advantage of the most well-protected avenue the people have to express themselves by providing rich open data to help us understand ourselves

Security, Transparency of the Audit

- Robust audits are fundamental to election integrity
- Officials must publish, or at least commit to, the data they plan to audit before random selection
- Easy to at least commit to it: e.g. ColoradoRLA publishing hashes on audit center (sometimes too late....)
- Widespread failure to do so undermines audits and confidence

Goal: Secure the chain-of-custody of paper ballots of record

- We must protect paper ballots - our only cyber-secure record of voter intent
- They must be protected from when they leave voter until audit, certification, years later
- No one I know is providing easy-to-verify evidence about the security of their chain-of-custody
 - 24x7 online videos are hard for citizens to validate as trustworthy
 - Hard to identify any tampering

Solution: commit to ballot images, check during audit

Great mitigation via ballot images:

- Publish a hash of each image as soon as possible after scanning
 - Seconds? Hours? A day?
- Label the hashes so they can be tied to the paper ballot card later on
- During the audit, pull the paper ballot and compare it to both the CVR and the image, and check the hash of the image.
- Various easy ways to publish the hashes and commit to them in a transparency log with any of a variety of ways to auditably authenticate whoever was publishing them.
Sigstore would be one easy way to Amazon Quantum Ledger Database (QLDB) *IETF Supply Chain Integrity, Transparency, and Trust (scitt) working group recently started up

Ballot images unsuitable for cyber-secure audit

- We can't fully trust ballot images, e.g. for audits, because they are not software-independent

Pattern voting attacks are highly overrated

Preventing people from participating in coercion would require going back to voting only in the polling place, which we are getting further and further from

Publishing actual CVRs helps transparency

- Naturally, we want to prevent reidentification of ballots given other available data
- See [Preserving Anonymity of Cast Vote Record](#), a 2018 submission by John McCarthy, Neal McBurnett, Harvie Branscomb, Ron Rivest, Philip Stark
- That public data should then be used in the audit
- Obfuscating data reduces public trust

Leveraging data for the public good

Huge opportunity which needs robust discussion:

- Perennial interest in data on all sorts of public opinion via polling, but increasingly hard to do
- Voting is the most widely used, well-protected avenue the people have to express themselves
- Take advantage of that by providing rich open data to help us understand ourselves

Leveraging data for the public good - 2

Unmasking just the audited CVRs via complicated crypto doesn't support these benefits of full CVRs available to the entire public

- Crystal-clear transparency and confidence-building for the large segment of the public which doesn't have a warm fuzzy feeling about cryptography
- Access to basic data like the residual vote, which homomorphic systems seem to require special tooling for I guess
- Support for independent tallies of arbitrary voting methods: RCV, Proportional Approval Voting, STAR-Voting etc.
- Easy computation of arbitrary statistics which may not be feasible with homomorphic systems.

Leveraging data for the public good - 3

- Research by political scientists of what various cohorts of the electorate actually want, including correlations across different contests,
- Research on historical elections to see how alternate voting methods would tally them

Open the floor for input

Note Adrian Fontes, SoS of AZ is supporting their bill for publication of CVRs, ballot images. Would like to hear more

I remember deep 2019 EVN online discussion, with insights from Stephanie Singer, Poorvi Vora, Harvie Branscomb, etc.

Open the floor for input from you all!