votingapp

Scan this code
for more information

Protecting Voter Privacy for Remote Voters

Abstract

Remote accessible add-on systems have provided military and overseas voters a method of voting remotely without having to deal with the pitfalls of mail delays and deployed first responders who are unable to receive and return a [1,2,3] mailed ballot. They have also been used for voters who are print-disabled, those for whom privately viewing or marking a paper ballot, or addressing an envelope, is impossible without sacrificing their privacy by requiring the assistance of others.

These systems, usually add-ons to existing voting systems, are often called "Electronic Ballot Delivery" and sometimes include "Electronic Ballot Return" features making the entire experience completely accessible.

More and more states are using these systems to complement their existing paper-based voting systems, especially as many transition to conducting "all-mail" elections, which eliminate the proliferation of accessible ballot marking devices at standard polling places.

Problem Statement

In-person, when a voter votes a paper ballot in a polling place or vote center, that voter signs a roster at which point they are given a paper ballot. The voter marks the ballot and drops that ballot into a ballot box or a precinct scanner. This is all done privately, as the ballot resides in a receptacle with all other ballots in that precinct and nothing ties a ballot to a voter's identity.

With most Electronic Ballot Delivery systems - that privacy is infringed. Usually with these systems, a voter will receive and mark a ballot electronically, then return it either by mail, fax, as an email attachment and in some cases they can submit the ballot online. The voter's signed affidavit, which is still connected to the voter's ballot either in an envelope or as a complete electronic document, is used to verify the validity of the signature.

Once the signature is verified, the ballot gets tabulated. However because the signature and the ballot are colocated, an election worker can effectively match a voter's identity to their vote. This is why many Electronic Ballot Delivery affidavits make voters aware that they are giving up their privacy when they vote using this method.

Background

When standard physical mail or absentee ballots are delivered to a voter, there are a variety of privacy protections that can be put in place. A separate signature envelope is often delivered with the paper ballot, so that the signature can be verified by one election worker prior to ballot extraction. A physical "security sleeve" can also be delivered with a ballot package, allowing the voter to place the ballot in the sleeve prior to inserting it into the signature envelope. This represents another layer of privacy for the mail voter during ballot extraction.

Unfortunately, these tools can not be used with Electronic Ballot Delivery systems, because of the fact that their delivery method is paperless. As mentioned above, the audiences for these systems are:

- **Military and Overseas Voters** - so they can receive and submit their ballots on-time without having to worry about mail delays.
- **Deployed First Responders** - who are unable to receive mail or vote in-person due to last minute emergency deployments.
- **Print-Disabled Voters** - for whom paper itself is inherently inaccessible.

votingapp

Scan this code
for more information

Solution

As jurisdictions look for Electronic Ballot Delivery (EBD) solutions, voter privacy can and should be prioritized. Thanks to new technology, it is possible to provide voters with an electronic ballot delivery system that does not tie the individual voter information with the marked ballot data for processing.

How Voter Privacy Is Protected:

- Jurisdictions use an air-gapped security device to that produces cast vote records that are not tied to a specific voter.
- Post election, the election official verifies signatures from the EBD Solution match the stored signatures in their voter registration system.
- The official then inserts an export from the EBD Solution into the air-gapped security device.
- The device provides the marked ballot data of all voters whose signatures were approved in an anonymous fashion.
- The official then takes the marked ballot data, remakes the ballots onto scannable stock, and scans them into their standard voting system, with the reassurance that their voters' privacy was protected.

Conclusion

As states implement Electronic Ballot Delivery and Return systems for their military and overseas voters, deployed first responders and voters with print-disabilities, protecting voter privacy should not be overlooked. Now that the technology exists, the ability to have completely anonymous ballots should be of paramount importance when selecting these systems.

References

For more technical information on how VotingApp protects voter privacy, read our white paper: End-to-End Verifiability with VotingApp.