Denial of Democracy: Voter Fraud in the Books

Emily Liu
Comp 116, Fall 2019

Abstract

When America talks about voter fraud, it's usually about "millions of people who voted illegally"[1]: an unbased claim that hordes of criminals wrongfully vote, despite their ineligibility. In the spectacle of such outlandish accusations, we've forgotten that illegal voting is actually the least of our concerns; the real issue with voter fraud lies in voter registration databases and electronic pollbooks. Between spotty availability and exposed voter information, although e-pollbooks provide for increased convenience for poll workers and voters alike, the security risks are significant enough to warrant a return to — or at least preservation of — paper records. This paper will focus on elections in the United States.

Introduction

Voter fraud, also known as election fraud, is any interference with the election system, typically through compromising vote accessibility and verity. While ballot and tallying machines are responsible for ensuring the accuracy of an election and are thus primary targets of election interference, pollbooks are equally important players in allowing people to vote at all, and need to be treated as such.

As electronic voting machines gain popularity, so do electronic pollbooks — but only one of these are held to a high standard of security. In some states, e-pollbooks have replaced paper records to show who's registered to vote at a certain location and to assist in the check-in process. There are some benefits. If someone goes to the wrong location, they can be easily redirected; if a state allows same-day registration, that can be done through the electronic system; in sixteen states, people can go to vote centers, where they are registered regardless of address.

But the same system means insecure or ineffective voter records. Online registration databases are left exposed to hackers who can view, modify, or even delete voter registrations. This violates the rights of citizens to vote, and to do so with anonymity. And even if the data is left untouched by election day, internet-connected pollbooks can find themselves the target of attacks that prevent or slow down voter check-in — effectively stalling democracy.

When voter registration databases and the e-pollbooks that are derived from them are compromised, people can't vote: simple as that. And when people can't vote, the democratic process that the U.S. so prides itself on is nonexistent.

---

[1] https://twitter.com/realDonaldTrump/status/802972944532209664

To the Community

We live in a time when it's common to keep personal information online: just today, I've submitted my address, credit card number, birthday, and cellphone number electronically. If someone tampered with or had access to this information, I wouldn't get my UberEats dinner and *might* have to cancel my card. But if someone were to tamper with my voter registration data, preventing me from entering the voting booth, I would become disenfranchised: effectively revoked of my right and responsibility as a citizen. And when large groups of voters are disenfranchised, it can sway elections, both local and federal, influencing governmental representation and legislation for years until the next one — impacting far more people than just American adult citizens. It's undeniable that the United States government is a major player on the world stage, so when that government is elected by a non-representative body, its false mandate affects everyone.

Background

In order to vote in an election in-person, an eligible adult American citizen needs to do three things: register to vote, check in at the polling station, and cast their ballot. To do the first two things, states are required to build and maintain a single centralized digitized database of voters, as per the Help America Vote Act of 2002,[2] which converts to the record with which poll workers check people in on election day. These databases contain name, birthday, address, registration status, and party affiliation. Their computerized format makes it far easier to register to vote online (available in 37 states as of October 2019), and has also allowed for an increase in popularity of electronic pollbooks.

Typically, poll workers use a pre-printed paper record of eligible registered voters for their precinct, used for look-up, verification, and check-in at the polls. When an adult citizen arrives to vote, their identification needs to be cross-checked with this giant binder to make sure they are registered at that station, and that they haven't already voted by absentee ballot. These e-pollbooks serve the same function as their analog counterparts, but have the additional benefits of real-time database updates. They rely on internet connectivity to maintain a unified accurate record across the state.

The 2018 elections saw 26.2% of districts using e-pollbooks — a 48% rise from the 2016 election. Of those districts, 97.6% used e-pollbooks to check-in voters, while 87.9% used them to look up polling locations, 85.7% used them to change voters' information, and around 14.8% used them for same-day registration.[3] In short, electronic pollbooks are on the rise.

Benefits

[2] 107th Congress. "Help America Vote Act of 2002"
[3] U.S. Election Assistance Commission. "Election Administration and Voting Survey"

The benefits of a digitized voter database are the same as any digitized record-keeping system, but with a literally national (and indirectly international) impact. With a centralized database and the live-updated e-pollbook it provides, the benefits are typically as follows:

- Faster check-in on election day: A computer is going to be much faster at looking up a registered voter than a human. Election day in the U.S. is inexplicably still not a federal holiday and polls close as early as 6 p.m. in some states, so for the people who can't leave work until 5 p.m., every second counts between getting through the door and reaching the ballot box.
- Redirection for voters: Often voters may go to the wrong location, either because their assigned polling station is farther from their home or work, or just out of confusion. Under the paper system, poll workers may only have access to voter records for people registered at that location, but with an e-pollbook it's just a quick search to correct any confusion.
- Voting centers: Currently, 16 states are even eliminating some local precinct assignments and opting for vote centers instead.[4] Vote centers are consolidated polling stations; voters can show up to vote at any, regardless of their home address. The electronic pollbook contains their registration information, and the networked system will update across all centers when the voter checks in.
- Same-day registration: In the 21 states that allow same-day registration as of June 2019, e-pollbooks are useful in checking identification and ensuring that the person did not vote already, for people who may have forgotten to register online or whose registration may have been accidentally (or maliciously) deleted or modified.[5] The analog option would be to provide a provisional ballot, and check afterwards if the person's vote is legitimate: it might not be counted.

The main benefits of electronic pollbooks are all geared towards making the voting experience as streamlined and convenient as possible for voters. It's a noble cause and significant effort: the internet makes it impossibly easy to hear everyone else's opinions, so why not use the same technology to vote your own?

Vulnerabilities

While migrating the electoral system towards a paperless future is attractive, the convenience it offers is not without vulnerability. Recall that the first two steps towards successful voting at a polling station are registration and check-in. The database that collects registrations is vulnerable to confidentiality and integrity violations, and the e-pollbooks for check-in are subject to DoS attacks egregious enough to turn away voters entirely.

[4] National Conference of State Legislatures. "Vote Centers."
[5] National Conference of State Legislatures. "Same-Day Voter Registration"

When an adult citizen registers to vote, they provide at least their name, address, political affiliation, and driver's license or social security number. This information is kept in the voter database mandated by the Help America Vote Act of 2002, as described above. The problem is that these online voter registration databases aren't secure — a quick query to the Massachusetts Voter Registration Search[6] with just a name, birthday, and zip code allowed me to find my mother's address, party enrollment, and voting status (she's registered). I got her permission to do so before trying, but I am not convinced that privacy-neglecting hackers would have the same level of decorum.

Ahead of the November 2018 midterm elections, the MIT Technology Review reported that U.S. special counsel Robert Mueller alleged that Russian hackers broke into the website of an undisclosed state's board of elections in 2016, accessing driver's license and partial Social Security numbers for about 500,000 voters.[7] The Associated Press recalled that the Illinois databases were compromised in July 2016, with hackers viewing (but not modifying or deleting) 76,000 active voter registration records.[8] And at DEF CON 2017, hackers playing with an e-pollbook sold on EBay found 654,517 records for voters in Shelby Country, Tennessee: name, address, birthday, political party, and whether they voted absentee.[9] It wasn't revealed what had happened technically in those hacks: whether they were due to SQL injection, compromised credentials, simply searching for a person's status like I did, or a combination of all three. But at DEF CON, it was simply a researcher finding a non-password-protected, unencrypted, removable memory card. Thus, across the three examples, at least a million voters have lost their right to privacy and confidentiality.

The integrity of voter information is also at risk. The Illinois hackers may not have modified database information, but that isn't to say nobody could. In a New York Times Magazine feature titled "The Crisis of Election Security" published ahead of the 2018 midterms, the author claims that hackers "could target voters themselves by deleting their names from the voter roll and electronic poll book … Or change their precinct assignments to send them to the wrong location, creating chaos and frustration that causes them to leave without voting."[10] This is what happened in the California June 2016 primary, when at least twenty voters were barred from voting because their party affiliation had been changed.[11] In these cases, voters had to either fill out a provisional ballot, or just go home having been denied their civic duty. When voter information is compromised, it can literally deprive democratic citizens of their most basic right.

This brings us to the last third of the CIA triad: accessibility. This is perhaps the most pervasive issue with electronic pollbooks: network unavailability, either via shoddy WiFi or good old-fashioned Denial-of-Service attacks. E-pollbooks need to be connected to the internet or an election board's network, according to an NPR podcast referencing Joseph Lorenzo Hall, Chief

[6] https://www.sec.state.ma.us/voterregistrationsearch/
[7] Giles (MIT Technology Review). "Four big targets in the cyber battle over the US ballot box"
[8] Sarah Zimmerman (Associated Press). "Illinois protecting against Russian election tampering"
[9] Kevin Collier (Gizmodo). "Personal info of 650,000 voters discovered on poll machine sold on EBay"
[10] Kim Zetter (The New York Times Magazine). "The Crisis of Election Security"
[11] John Sepulvado (KQED). "DA: Hackers Penetrated Voter Registrations in 2016 Through State's Election Site"

Technologist at the Center for Democracy and Technology.[12] Connectivity is necessary for the pollbooks to talk to each other about who has voted already and where, to prevent anyone from casting multiple ballots. But this also leaves e-pollbooks exposed to DoS attacks, which can halt check-in and annoy voters into leaving. We've already seen examples of poorly connected pollbooks slowing check-in and turning off voters: North Carolina in 2016,[13] Minneapolis in 2017,[14] South Dakota in 2018,[15] and Johnson County, Indiana in 2018.[16]

In most cases above the assumed reason for stalling was lack of bandwidth, but it's not outlandish to think that a large number of requests (malicious or otherwise) to the e-pollbook networks would have the same result. And, while the above examples were not confirmed to be intentional DoS targeting, attacks on other parts of the electoral system show that this kind of attack is not out of the question: in the Knox County, Tennessee 2018 primaries, the election-reporting website was overwhelmed with a confirmed DDoS attack, leading to widespread panic about the electoral system being "down."[17] Even though the actual voting numbers were not compromised, it is clear that the election system is a prominent target of such malicious actions.

Besides the obvious interruption to the electoral process, these vulnerabilities provoke an even more insidious obstruction to our democratic system. Americans lose their political efficacy: faith in government and belief that their vote matters. Difficulties in the voting process lead to exasperation and distrust in the legitimacy of elections, and can cause lower voter turnout in the future, thus rendering useless the very purpose of democracy.

Action Items

My first recommendation is to incorporate two-factor authentication for checking and modifying voter registration status online. Name, birthday, and zip code are simply not sufficient to protect your home address and party affiliation. Anybody from Facebook friends to UberEats to staffers on political campaigns can figure out birthday and zip code and thus party affiliation — even if it's not quite as high-stakes as medical history or credit card statements, everyone has a right to keep that information private. This two-factor authentication would require voters to come up with a password to check their status, and a second mode. Duo would be ideal, but it's not necessarily accessible for all citizens of varying financial statuses, so we may have to settle for texts or email: still better than birthday and zip code.

The centralized registration databases should be encrypted as well, if not already. This applies to any data kept on the actual e-pollbook itself, so we don't get a repeat of the DEF CON exploit. Also

[12] Miles Parks (NPR). "Technology Has Made Voting Lines Move Faster But Also Made Elections Less Secure."
[13] Pam Fessler (NPR). "Russian Cyberattack Targeted Elections Vendor Tied To Voting Day Disruptions"
[14] Mary McGuire (CBS Minnesota). "Minneapolis Voters Encounter Problems with New E-Pollbooks."
[15] Stewart Huntington (KOTA TV). "Software failure mars election night here and in 8 other counties."
[16] Voting System Technical Oversight Program. "A Preliminary Investigation of ES&S Electronic Poll Book Issues in Johnson County, Indiana for the 2018 General Election."
[17] Center for Democracy and Technology. "Election Cybersecurity 101 Field Guide: DDoS Attack Mitigation."

on the e-pollbook: the memory card shouldn't have been left in the machine anyways, but since it was, all voter profiles on the card should be password-protected so only pollworkers can access it.

In the cases of potential denial-of-service attacks on the pollbooks, the e-pollbook servers should keep track of all IP addresses used for requests, and limit responses only to IP addresses known to be actual e-pollbooks owned by the state. And in case the DoS attacks prevail, all polling stations should keep or continue to keep paper backups instead. According to a Pew Charitable Trusts infographic (Fig. 1), of the 27 states using some form of electronic pollbook, only 17 keep backup paper rolls on hand. And of those same 27 states, only 16 have a written security protocol (Fig. 2). [18]

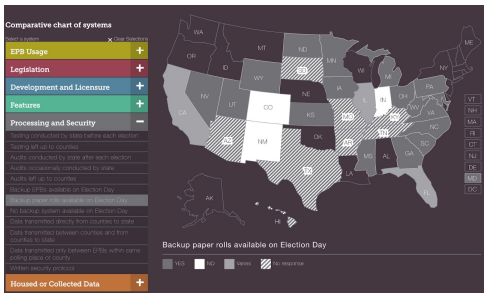

Figure 1.

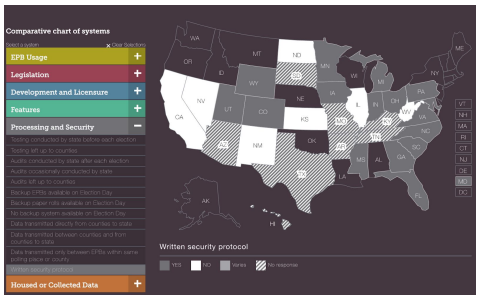

Figure 2.

There are also some pushes to create new systems entirely for a technologically-advanced election. For example, Galois has come out with a "Free & Fair ePollbook" project: "a scalable, secure and resilient electronic poll book solution for precinct polling places and county vote centers."[19] While it's not entirely clear what exactly makes the e-pollbook so secure, this project, in conjunction with their ElectionGuard electronic voting machine software, make for a noble push into the right direction of revamping the whole electoral system.

Conclusion

Overall, I'm optimistic about the future of voter databases and electronic pollbooks. Computer science, software engineering, and the internet were not exactly designed to be secure, but I believe that after the myriad vulnerabilities exposed and attacks witnessed on e-pollbooks since 2016 onwards, policymakers and technologists alike understand the urgency of a complete overhaul and securing of our electronic voting system. It's true that e-pollbooks provide greater ease in the democratic process, but they should not be allowed to do so at the expense of voter confidentiality, data integrity, and democratic accessibility. We need a new system that is secure from end to end; from registration to check-in to ballot submission itself. And even with a wholly redesigned system? Computer scientists know: We should still be prepared to use paper.

[18] Pew Charitable Trusts. "A Look at How — and How Many — States Adopt Electronic Poll Books"
[19] Galois. "Galois Launches Election Technology Spinoff: Free & Fair To Enable Verifiable, Transparent and Secure Elections"

Works Cited

107th Congress, Public Law 107–252. "Help America Vote Act of 2002." https://www.govinfo.gov/content/pkg/PLAW-107publ252/pdf/PLAW-107publ252.pdf

Center for Democracy and Technology (CDT). "Election Cybersecurity 101 Field Guide: DDoS Attack Mitigation." https://cdt.org/insights/election-cybersecurity-101-field-guide-ddos-attack-mitigation/

Collier, Kevin. Gizmodo. "Personal info of 650,000 voters discovered on poll machine sold on EBay." https://gizmodo.com/personal-info-of-650-000-voters-discovered-on-poll-mach-1797438462

Fessler, Pam. National Public Radio (NPR). "Russian cyberattack targeted elections vendor tied to voting day disruptions." https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions

Giles, Martin. MIT Technology Review. "Four big targets in the cyber battle over the US ballot box." https://www.technologyreview.com/s/611813/four-big-targets-in-the-cyber-battle-over-the-us-ballot-box/

Galois. "Galois Launches Election Technology Spinoff: Free & Fair To Enable Verifiable, Transparent and Secure Elections." https://galois.com/news/galois-launches-election-technology-spinoff-free-fair-enable-verifiable-transparent-secure-elections/

Huntington, Stewart. KOTA TV. "Software failure mars election night here and in 8 other counties." https://www.kotatv.com/content/news/Software-failure-mars-election-night-here-and-in-8-other-counties-484783791.html

McGuire, Mary. CBS Minnesota. "Minneapolis Voters Encounter Problems with New E-Pollbooks." https://minnesota.cbslocal.com/2017/11/07/minneapolis-voters-e-poll-problems/

National Conference of State Legislatures. "Same Day Registration." http://www.ncsl.org/research/elections-and-campaigns/same-day-registration.aspx

National Conference of State Legislatures. "Vote Centers." http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx

Parks, Miles. National Public Radio (NPR). "Technology Has Made Voting Lines Move Faster But Also Made Elections Less Secure."

https://www.npr.org/2019/05/30/727529802/technology-has-made-voting-lines-move-faster-but-also-made-elections-less-secure

Pew Charitable Trusts. "A Look at How—and How Many—States Adopt Electronic Poll Books." https://www.pewtrusts.org/en/research-and-analysis/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books

Sepulvado, Jon. KQED. "DA: Hackers Penetrated Voter Registrations in 2016 Through State's Election Site." https://www.kqed.org/news/11579541/hackers-penetrated-voter-registrations-in-2016-through-states-election-site

U.S. Election Assistance Commission. "Election Administration and Voting Survey." https://www.eac.gov/assets/1/6/2018_EAVS_Report.pdf

The Voting System Technical Oversight Program (VSTOP). "A Preliminary Investigation of ES&S Electronic Poll Book Issues in Johnson County, Indiana for the 2018 General Election." https://www.in.gov/sos/elections/files/Report%20-%20Johnson%20County%20ePB%20Investigation%20Dec%2031%202018.pdf

Zetter, Kim. New York Times Magazine. "The Crisis of Election Security." https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html

Zimmerman, Sarah. Associated Press. "Illinois protecting against Russian election tampering" https://apnews.com/6e21221f5f934ce4bffc39cc788b9810