Contact: mikefarb@unhackthevote.com
@mikefarb1

Voter Registration Databases: Targets

Updated 9 December 2017

PART I – The Motive

It is an established fact that Russia targeted the voter registration databases[1] during several months leading up to and following the 2016 election.

What is a voter registration database, you ask?

Voter Registration Rolls, Lists, and Databases

The National Voter Registration Act (NVRA)[2] of 1993, among other things, protects the integrity of the electoral process and ensures that accurate and current voter registration rolls are maintained.

The federal Help America Vote Act (HAVA)[3] established in 2002 requires all states to establish statewide voter registration lists,[4] which "serve as the official voter registration list for the conduct of all elections for Federal office in the State."[3,4] Voter registration lists are implemented by each state, "acting through the chief State election official."[3] These include personal information[5] such as names, birthdates, addresses, and contact information, and a unique identifier. Per HAVA, "Any election official in the State, including any local election official, may obtain immediate electronic access to the information contained in the computerized list."[3]

The NVRA establishes rules and guidelines for states to maintain voter registration rolls. States are responsible for ensuring voter registration rolls are accurate and up to date. [2] States have discretionary authority[6] to *add to* the NVRA requirements for voter roll maintenance, but the NVRA establishes a minimum standard that all states must implement. Similarly, HAVA leaves methods of compliance to discretion of states:[3]

> **§15485. Methods of implementation left to discretion of State**
>
> The specific choices on the methods of complying with the requirements of this subchapter shall be left to the discretion of the State.
> (Pub. L. 107â€"252, title III, §305, Oct. 29, 2002, 116 Stat. 1714.)

States use data from federal or state agencies or other states to check the accuracy[4] of their voter registration lists, such as using information from the United States Post Office, the Social Security Administration, and the Department of Homeland Security.

Contact: mikefarb@unhackthevote.com
@mikefarb1

VOTER LIST ACCURACY

6/16/2016

All states take steps to keep their voter registration rolls accurate and up-to-date. The goal of maintaining an accurate voter list is to prevent ineligible people from voting, prevent anyone from voting twice and, by reducing inaccuracies, speed up the voter check-in process at polling places. How states do this can vary, but most have processes in place for removing records of duplicate records, deceased voters, felons and people who have moved. These checks can be conducted with data from federal agencies, state agencies, or other states.

From NCSL.org[6]

FUN FACT

Citizens must be registered to vote in all states except North Dakota,[4] which allows voting (with proper identification) with no advance registration.

The NVRA defines criteria that allow a voter to be removed[6] from voter rolls. Per HAVA, maintenance of voter registration lists shall ensure "duplicate names are eliminated from the computerized list."[3] This maintenance process can be different for each state.

In many states, the state election agency may "cross-check" computerized voter registration list information with other state agencies,[6] such as departments that handle vital statistics and records for motor vehicles, deaths, felons, and jury duty. Some states participate in an interstate cross-check program[6] for maintaining voter registration lists. Participating states currently send their data to Kansas, where the data are reviewed, and states receive a list of identified potential duplicate registrations. Investigative reporters like Greg Palast have written extensively on cross-check,[7] finding that the program is significantly flawed.

NOT-SO-FUN FACT

The cross-check program was found to be in error over 99% of the time.[8]

This anti-voter-fraud program gets it wrong over 99 percent of the time. The GOP wants to take it nationwide.

From Washington Post[8]

Computerized voter registration lists are frequently stored in electronic database programs.[9] Thus, you'll often hear the term "voter registration databases" referring to the computerized voter registration lists defined in HAVA.

What is a Database?

Here's a video that helps explain what a database is, and how it works:
https://www.youtube.com/watch?v=eXiCza050ug

Security of Voter Registration Databases

HAVA requires State or local election officials to provide security for voter registration lists, but the requirements are general, i.e., essentially a performance goal.[4]

> **(3) Technological security of computerized list**
>
> The appropriate State or local official shall provide adequate technological security measures to prevent the unauthorized access to the computerized list established under this section.

In the Caltech Institute of Technology (Caltech) Election Updates Blog,[10] Michael Alvarez @rmichaelalvarez, professor of political science at Caltech and co-director of the Caltech/MIT Voting Technology Project (VTP) writes: "The potential threats to state voter registration databases have been known for a long time." Michael published Potential Threats to Statewide Voter Registration Systems[11] in October 2005, as part of the VTP. Michael identified several potential issues with computerized voter registration lists:

- Computerized voter registration lists are stored and maintained in a single centralized system, i.e., a "single place where attackers can focus their energies."
- There are no existing standards for these computerized lists or databases, and there is no corresponding testing and certification process to ensure that the databases comply with such standards.

Michael identified four categories of threats to voter registration lists, which were still of concern in 2016:[10]

- Authenticity of the registration file: attacks on the transmission path of voter registration data from local election officials to the state database, or attacks on the transmission path of data between the state registry to other state officials (for example, departments of motor vehicles).
- Security of personal information in the file: state voter files contain a good deal of personal information, including names, birthdates, addresses, and contact information, which could be quite valuable to attackers.
- Integrity of the file: the primary data files could be corrupted, either by mistakes which enter the data and are difficult to remove, or by systematic attack.
- System failure: the files could fail at important moments, either due to problems with their architecture or technology, or if they come under systematic "denial of service" attacks.

From Michael Alvarez, Caltech[10]

In short, there are multiple ways that voter registration files and databases can be compromised.

Focusing on Michael's first identified threat above, authenticity of the registration file, reveals multiple points of contact where the information could be hacked or compromised, such as:

- storage/maintenance locations at local election offices;
- points along the data transmission path between local and state election officials;
- storage/maintenance locations at the state level;
- points along the data transmission path between multiple agencies, such as for comparison to DMV, social security, or cross-check databases; and
- storage/maintenance locations at these other agencies.

Authenticity of the registration file

A first threat to authenticity of the statewide voter registration file arises due to the centralization of the voter registration list. The new centralized statewide voter registration systems required by HAVA will involve some form of data transfer between the local election officials, who in many states will retain some responsibility for the voter registration data and who will need the voter registration data for a wide range election administration tasks. This means that these statewide systems will involve voter registration data being passed from state to localities, which implies new points of vulnerability --- during the data transmission process and in the local election office. So while there is a centralized statewide list, it is possible that attackers could isolate points of vulnerability in the transmission path, or in one of many local election offices and possibly access the state list via local vulnerabilities that might be outside the direct control of state election officials.

Second, the statewide voter lists will be interactive with other databases, as required by HAVA, in particular state Department of Motor Vehicle and Social Security Administration databases. Again, the statewide voter data will be transmitted for comparison to those lists, and thus again be potentially vulnerable in transmission and when in places potentially outside the state election official's control. There has also been much talk recently about potential interoperability of statewide voter registration lists between states, which depending upon how implemented again may open the door for new vulnerabilities not experienced in the former decentralized voter registration systems in place throughout most of the nation before the passage of HAVA.[3] Thus, these potential vulnerabilities imply that attackers could have access to voter registration information and the ability to alter that information or add entries to the file.

From Michael Alvarez, VTP[11]

We have seen significant failures in security of voter registration databases in recent years. In December 2015, Reuters reported that a database with information on 191 million American voters[12] was accessible on the internet due to improper security protocols for a voter registration database.

The database includes names, addresses, birth dates, party affiliations, phone numbers and emails of voters in all 50 U.S. states and Washington, researcher Chris Vickery said in a phone interview.

From Reuters[12]

It is unknown who may have downloaded and subsequently distributed the database, which could be weaponized, including for purposes of committing election fraud.

> While voter data is typically considered public information, it would be time-consuming and expensive to gather a database of all American voters. A trove of all U.S. voter data could be valuable to criminals looking for lists of large numbers of targets for a variety of fraud schemes.

From Reuters[12]

Russia Targeted Voter Registration Databases

In September 2017, the Department of Homeland Security (DHS) notified at least 21 states,[13] for the *first time*, that their voter registration databases were targeted *a year ago* by Russian government hackers.

> The U.S. Department of Homeland Security is reiterating that it believes 21 states were the target of Russian government hackers seeking vulnerabilities and access to the U.S. election infrastructure.
>
> Sept. 26, 2017, at 10:11 p.m.

AP

> MADISON, Wis. (AP) — The Latest on Wisconsin Elections Committee meeting to discuss attempted Russian hack (all times local):
>
> 9:05 p.m.
>
> The U.S. Department of Homeland Security is reiterating that it believes 21 states were the target of Russian government hackers seeking vulnerabilities and access to the U.S. election infrastructure.

From AP News[14]

In June 2017, DHS stated that the Russian government attempted to hack voter registration lists or public election sites in 21 states during the 2016 election. However, state election officials were not notified until three months later, in September 2017, that they were targeted.[14] Why were states not notified until a year after the attacks occurred?

> State elections officials in Alabama, Colorado, Connecticut, Iowa, Maryland, Minnesota, Ohio, Oklahoma, Pennsylvania, Virginia, Wisconsin and Washington were told Friday they were targeted, according to officials and a tally by the Associated Press.

From Washington Post[13]

As noted above, maintenance of voter registration databases is the responsibility of election officials in each state. If states were not notified until September 2017 that they were being targeted, what basis would DHS have for testifying in June that 21 states had been affected but vote-tallying machines were unaffected? What manner of investigation could have been conducted by DHS without notifying and working with state election officials, who are responsible for maintaining both voting machines and voter registration databases?

It appears the DHS reviewed activity of suspicious IP addresses targeting state election systems, in attempts to "scan" voter registration databases. However, the DHS itself stated that review of IP addresses alone might not show the full picture of Russia's efforts to target voter registration databases.

> But later Tuesday Homeland Security spokesman Scott McConnell told The Associated Press in a statement that "discussions of specific IP addresses do not provide a complete picture of potential targeting activity."
>
> From AP News[14]

Why Would Russia Target Voter Registration Databases?

Why were voter registration databases targeted? How could hacking a voter registration database be part of hacking an election?

The most obvious answer is disenfranchisement. If voters are deleted from voter registration databases, or if their address or identifying information is changed in such a way that they don't show up in the poll books when they attempt to vote, they may cast a provisional ballot, or simply walk away confused, without casting a vote.

A recent article in the Christian Science Monitor[15] by Warren Richey[16] highlights this potential danger.

> But there is evidence of repeated attempts to break into another critical part of the election system: voter registration rolls.
>
> The implications are potentially severe. Whoever controls the list of registered voters, controls who gets to vote.

Hacking and/or altering voter registration databases is a significant act. It's highly unlikely this would be done without a specific outcome in mind. As we note above, voter registration lists include specific, personal information. Altered information in the databases, and the resulting disenfranchisement, could strategically target specific groups of voters based on gender, race, address, political party, or other criteria in an attempt to suppress their votes.

Disenfranchisement could be a "tasty meatball" for someone attempting to influence election outcomes. However, there are multiple ways hacked voter registration databases can be used in an election.

Warren Richey identifies another, even more ominous, way that an altered registration database could contribute to election hacking.

> There are easier ways to fix an election, but experts acknowledge that a large number of deceased or otherwise dormant voters on a registration list could help give cover to a malicious attack that might be exceedingly difficult to detect.

Inactive voters remaining on a registration list can be used to hide election fraud. What if the status of the inactive voters was suddenly converted to active? How could these newly active "zombie" voters be used? Could their numbers be used to falsely inflate totals of registered voters for a specific party? Could they be included in totals used to manipulate the narrative regarding voter turnout? Could electronic votes be recorded in the system as if they were cast by these zombie voters?

HAVA[4] specifically requires states to ensure voter registration lists are accurate and updated regularly, including reasonable efforts to remove ineligible voters.

> **(4) Minimum standard for accuracy of State voter registration records**
>
> The State election system shall include provisions to ensure that voter registration records in the State are accurate and are updated regularly, including the following:
> (A) A system of file maintenance that makes a reasonable effort to remove registrants who are ineligible to vote from the official list of eligible voters. Under such system, consistent with the National Voter Registration Act of 1993 (42 U.S.C. 1973gg et seq.), registrants who have not responded to a notice and who have not voted in 2 consecutive general elections for Federal office shall be removed from the official list of eligible voters, except that no registrant may be removed solely by reason of a failure to vote.
> (B) Safeguards to ensure that eligible voters are not removed in error from the official list of eligible voters.

Are all the states complying with this requirement? How many states are leaving ineligible voters in their voter registration databases?

As with any sophisticated crime, there is a second part: the cover-up.

Hiding Hacking of Voter Registration Databases

When most people think of "election hacking" they think of vote totals being changed, such as by hacked electronic machines flipping vote totals as voting occurs, or hackers later changing the information stored on individual voting machines, or even hackers altering tallies electronically. These activities could be easier to accomplish, particularly on a smaller scale, such as for a specific precinct, within a state, or for a specific type of voting machine, regardless of its location. These types of hacks could be enough to alter an election outcome when smaller numbers of votes make the difference between winning candidates. These kinds of hacks might also fly under the radar if voter registration databases are not altered to help with the cover up.

The Reuters article[12] notes that voter registration information could be used to commit fraud, and Richey[15] notes that inactive voters remaining in voter registration databases could be used to cover up election fraud.

Following what we could jokingly call the "Law of Laziness", people do the minimum needed to achieve the objective. It's just practical. Hacking and altering information in a voter registration database is a high-difficulty, high-risk activity. So, why not stick to the easier hacks described above? Likely *because they needed to*. Hacking voter registration databases may have been the minimum needed to achieve the objective of altering the outcome of the election. This bigger hack offers the potential to manipulate and control large numbers of votes, paired with the ability to mask the activity by tweaking the voter registration database. Change a few numbers, manipulate the totals everyone looks at and talks about, control the narrative. It's high-risk, high-reward for nefarious entities who intend to commit election fraud.

Anyone changing vote totals, altering voter registration information, and altering election outcomes surely would want to avoid detection and make us think nothing really happened. Blatant election fraud would risk having the falsified election result challenged and nullified, and could have severe consequences. Easily detectable manipulation of voter registration databases blows the secrecy of the hack, burning it as a covert operation, so it cannot be used again in the future.

To hide a massive hack like altering information in voter registration databases, the hacker must first change vote totals in some way, then create an explanation to keep us from rethinking our election systems and ending the game for good. The intent would be to create falsified data that people would believe are reasonable, implying the election results are real and there is some reasonable explanation for what occurred. If changes were made to voter registration database information, these must seem valid. Changing demographics? Disgruntled or apathetic voters? Nothing to see here. Please move along.

We rely on voter registration lists to give us information about voters. How many are registered in each precinct? Are they Democrats? Republicans? Not affiliated with either major party? How many voters went to the polls? Was there low turnout in some areas? Higher turnout in others? Registration data answers these questions, and the answers to these questions help support explanations for unexpected outcomes. In the case of the 2016 presidential election, researchers and journalists turned to registration data to make sense of the unexpected outcome.

Voter registration databases serve as a control on votes that are allowed to be cast. Not in the voter registration file? No vote. However, any individual in the database, listed as an actively registered voter, with a unique voter ID, can cast a vote.

What if some voters were disenfranchised through altered data in voter registration lists, thus preventing them from voting or causing them to cast provisional ballots that may or may not have been counted? What if the voter registration databases were manipulated? What if the voter data and various totals we all use to summarize what happened during the election, which we all accepted as valid, were false?

What if "zombie" voters were also added to the voter registration databases in order to alter apparent demographics?

Voter registration databases have the potential to be mighty weapons for those seeking a high-risk, high-reward way to manipulate the outcomes of elections.

Sources

Sources are hyperlinked throughout.

1. http://time.com/4828306/russian-hacking-election-widespread-private-data/
2. https://www.justice.gov/crt/title-42-public-health-and-welfare-chapter-20-elective-franchise-subchapter-i-h-national-voter
3. https://www.justice.gov/crt/help-america-vote-act-2002
4. http://www.ncsl.org/research/elections-and-campaigns/voter-registration.aspx
5. https://electionupdates.caltech.edu/2016/10/12/how-secure-are-state-voter-registration-databases/
6. http://www.ncsl.org/research/elections-and-campaigns/voter-list-accuracy.aspx
7. http://www.gregpalast.com/election-stolen-heres/
8. https://www.washingtonpost.com/news/wonk/wp/2017/07/20/this-anti-voter-fraud-program-gets-it-wrong-over-99-of-the-time-the-gop-wants-to-take-it-nationwide/?utm_term=.42c1946a8da8
9. https://www.britannica.com/technology/database
10. https://electionupdates.caltech.edu/2016/10/12/how-secure-are-state-voter-registration-databases/
11. http://vote.caltech.edu/working-papers/40
12. https://www.reuters.com/article/us-usa-voters-breach/database-of-191-million-u-s-voters-exposed-on-internet-researcher-idUSKBN0UB1E020151229
13. https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.ac8678130179
14. https://www.apnews.com/daefa94abee54d549bba87bfbdf8cb26
15. https://www.csmonitor.com/Daily/2017/20171103/Could-Henny-Nelson-age-131-help-Russia-rig-an-election
16. https://www.csmonitor.com/About/People/Warren-Richey

@KottiPillar
@Saill
#unhackthevote

PART II – The Opportunity

PART III – Who is Minding the Cradle?

PART IV – Our Investigation

PART IV – Our Findings

Companion Twitter Thread

Read @mikefarb1's companion thread on Twitter