THE TECHNOLOGICAL SECURITY OF AMERICAN ELECTIONS: DEFINING, UNDERSTANDING, AND IMPLEMENTING SECURE ELECTIONS IN AN INSECURE WORLD

by

MAXWELL H. TERRY

A THESIS

Presented to the Department of Computer and Information Science
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Science
June 2021

An Abstract of the Thesis of

Maxwell Terry for the degree of Bachelor of Science
in the Department of Computer and Information Science to be taken June 2021

The Technological Security of American Elections: Defining, Understanding, and Implementing Secure Elections in an Insecure World

Approved: *Michal Young, Ph.D.*
Primary Thesis Advisor

The topic of election security has dominated news cycles throughout the country in the wake of one of the most contentious elections in American history. As technology continues to develop, become more accessible, and integrate with electoral processes, each election cycle introduces new laws and ways for registered citizens to vote. We now see a diverse range of voting methods used throughout the country, such as vote-by-mail/absentee ballots, early voting, and even voting through an online portal for a select few Americans. Each separate method in each state/county utilizes different machines, security checks, and rules and regulations. With such a high degree of complexity comes questions about the technological security of American elections. In order to guarantee the fundamental democratic principle of fair and free elections, election security must be ensured such that each voter can be confident that their vote is counted as intended. Throughout the following sections I will highlight the technological risks inherent in the United States' core election infrastructure to make recommendations on how to further improve the technological security of American elections. I will accomplish this by defining core features of the electoral system,

including the different voting methods and machines used throughout the country. During this discussion I will address plausible security flaws in each method/machine's structure. I will show how these flaws could, and have, been exploited by detailing both studies conducted on voting machines/processes as well as the foreign and domestic security risks posed by the events of the 2016 presidential election. Finally, I will make recommendations on how to improve the technological security of elections throughout the country at each step of the electoral process.

Acknowledgements

First and foremost, I would like to extend a great deal of gratitude to my primary advisor, Professor Michal Young, for his continued support throughout the thesis process. When I was struggling to find an advisor to advocate for me at the end of my Junior year, Professor Young stepped up and helped me formulate my research. Additionally, I have worked under Professor Young as a computer science learning assistant for many terms, and he has always been there when I needed help or guidance. I would also like to thank my secondary advisor, Professor Priscilla Southwell, who has provided crucial insight into my discussions of American elections as a leading expert in the field. Her feedback, as well as her papers, have been integral to the structure and development of my thesis. Next, I would like to thank my Robert D. Clark Honors College representative, Professor Daniel Rosenberg, for meeting with me multiple times and helping me push my thesis in new directions.

Aside from my brilliant committee, I would like to thank Professor Kathleen Freeman from the computer science department. The first class I ever took in college was with Professor Freeman, and I have worked under her tutelage for the majority of my college career. Professor Freeman has had an immense impact on my life. Finally, I would like to thank my family for their unrelenting support. They are not only my greatest mentors, but also the most caring people I have had the pleasure of being with.

Table of Contents

List of Figures

Chapter 1: Background

Elections Clause

Article I Section 4 Clause 1 of the United States Constitution gives states the power to decide how to run their electoral processes. From voter registration and ballot collection to the counting of election results, each state has their own election regulations. Often referred to as the "Elections Clause," the Constitution reads:

> The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of choosing Senators.

An analysis of the Elections Clause reveals that the federal government leaves much of the power of deciding the "times, places, and manner" of voting in both federal and local elections to each individual state. The Constitution dictates that Congress can only override state laws through Constitutional Amendments such as the 15th Amendment, which guarantees the right to vote to all men regardless of "race, color, or previous condition of servitude."[1] Congress can also pass laws to pursue the goals stated in each Amendment, a famous example being the Voting Rights Act of 1965 which aimed to actualize the goals of the 15th and 19th Amendments. Federal courts up to the Supreme Court decide the Constitutional legitimacy of voting laws passed by Congress and the states.

Due to the nature of each independent state prescribing their own methods of voting, the United States ends up with an incredibly mixed bag of voting laws and processes employed throughout the nation. The largest degree of variance comes with

[1] U.S. Const. amend. XV. Sec. 1. cl. 1.

which machines or methods states use to collect, count, and store ballots, as well as how they transmit voting results. As an example, since 2000, Oregon conducts all elections through vote-by-mail systems while many other states, such as Louisiana and Mississippi, still vote almost entirely in-person.

With a high degree of complexity regarding how people vote from state to state comes an even higher complication for election security. Security must be guaranteed uniformly across the country, though the technology remains incredibly diverse. Though there are countless differences between states, there are still several common denominators. Regarding the methods employed to collect votes, all states use some varying combination of vote-by-mail systems and in-person voting that will be discussed throughout Chapter 2. Regarding the technology used throughout the election process, there are a few common machines that represent the vast majority of voters which will be the topic of Chapter 3. Observing commonalities between states reveals that there are several common security risks seen throughout the states. I will largely be discussing common security risks rather than focusing on each state's unique problems, as the common risks have the largest implications on American election security. How these common risks can be exploited by foreign and/or domestic actors will be the topic of Chapter 4. Recommendations to alleviate these common risks will be proposed and analyzed throughout Chapter 5.

Software Independence

The term "software independence" in the context of elections refers to a modern computer science approach to how voting systems should work. The term bases its meaning around the idea that software is fallible. Whether initially known or unknown,

every piece of software and hardware in the world contains inherent security risks. Thus, the term "software independence" used in the realm of voting machines means that, in all voting processes, software should not be the only system used to collect and tabulate votes.[2] Rather, there should be a blend of software and human functions to ensure accurate election results. The goal of software independence is to guarantee that an undetected error in a voting machine does not cause an undetected error in the election outcome. If each state's electoral processes practice the ideologies of software independence, errors incurred throughout the voting process have a higher likelihood of being caught and corrected before election results are finalized.[3]

Paper Trails

One tactic commonly used to ensure software independence is the maintenance of a verifiable "paper trail." In the context of electoral processes, paper trails are a physical product of each voter's ballot selections. This commonly takes the form of physical voter ballots collected within each precinct, but also refers to physical voter pollbooks and tangible outputs from voting machines, such as a paper voting receipt. Paper trails play into the idea of software independence as they promote the use of a physical medium to check against the results of software. When the results produced by computers need to be checked with scrutiny or cannot be trusted due to alleged insecurity, precincts can affirm or deny election results by auditing their paper trails.[4]

---

[2] Rivest, Ronald L. "On the notion of 'software independence' in voting systems." *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences* vol. 366,1881 (2008): 3759-67. doi:10.1098/rsta.2008.0149

[3] Ibid.

[4] US House of Representatives Committee on House Administration, and Matt Blaze. Document, 2020 Election Security - Perspectives from Voting System Vendors and Experts § (2020).

Both software independence and the production and use of paper trails are crucial metrics of election system security. Whether or not different voting mechanisms can reliably produce backups to affirm or deny election results is imperative to guaranteeing secure results. Machines should be viewed and utilized as a tool to aide elections without compromising the physical human components necessary to check the machine's work.

Chapter 2: Voting Methods

Introduction

Understanding the technological security of American elections means first understanding and analyzing the different major methods of ballot collection. There are two major categories of ballot collection used throughout the states: mail-in voters and in-person voters. While the method utilized and the exact specifics of their use differ between states, these two categories of voters can be used to invoke discussions about the security of ballot collection generally. Both methods are inherently linked to ballot collection/tabulation machines which will be discussed throughout Chapter 3.

Mail-In/Absentee Voting

Mail-in and absentee voting refer to the same process: a single voter is mailed a single ballot which, after the voter submits said ballot, undergoes rigorous scrutiny by machines and local election officials to ensure that the results reflect the intended selections of each eligible voter. A part of this process involves ensuring that each person votes only once. Mail-in only states, such as Oregon, send a single ballot to every registered voter. For states that largely vote in-person, absentee ballots are mailed out on an "excuse" or "no-excuse" basis. An "excuse" meaning the voter must provide a valid reason as to why they could not vote in-person on election day, whether it be due to age, disability, absence, or other condition. A few examples of states that utilized excuse absentee ballots in the 2020 federal election are Texas, Louisiana, and

Mississippi.[5] In states where excuses are not required, such as in California, any voter can request to vote-by-mail and will subsequently be sent a ballot.[6] In accordance with the Elections Clause, how the ballots are mailed out, received, checked for security, and counted differs from state to state.

Due to the prevalence of the COVID-19 pandemic, the 2020 election saw a distinct uptick in the number of states that allowed voters to mail-in ballots. In states that still required excuses for absentee voting, excuses surrounding the pandemic, such as having to quarantine, being at higher risk, or displaying symptoms, could be used to receive a mail-in ballot. This led to over 65 million voters casting mail-in/absentee ballots in 2020, nearly doubling the 2016 mark of 33 million Americans.[7] With such a stark increase in mail-in ballots, especially from states that traditionally have not allowed such widespread use, comes the question of whether the votes were truly secure. Past trends demonstrate that voting by mail is an incredibly secure system regardless of scale.

The Heritage Foundation consistently updates a running database of a sample of election fraud cases throughout the United States. As of the start of 2021, according to the sample there have been 1,317 proven instances of voter fraud over approximately 30 years, resulting in 1,134 criminal convictions.[8] Of these proven instances, just 213 have

[5] "Voting Outside the Polling Place: Absentee, All-Mail and Other Voting at Home Options." National Conference of State Legislatures, September 25, 2020. https://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx.
[6] Ibid.
[7] Desilver, Drew. "Most Mail and Provisional Ballots Got Counted in Past U.S. Elections – but Many Did Not." Pew Research Center. Pew Research Center, November 10, 2020. https://www.pewresearch.org/fact-tank/2020/11/10/most-mail-and-provisional-ballots-got-counted-in-past-u-s-elections-but-many-did-not/.
[8] "A Sampling of Recent Election Fraud Cases from Across the United States." The Heritage Foundation. Washington D.C. Accessed March 26, 2021. https://www.heritage.org/voterfraud/search.

come from the fraudulent use of absentee ballots. In the same time span, over 250 million mail-in votes have been cast. Such numbers show that 213 cases are statistically insignificant, even when taking into consideration the largest occurrence of mail-in voting in American history. Oregon, a state that has done all elections by mail since 2000, has documented approximately 12 cases of criminal voter fraud out of over 100 million ballots.[9] Most of these cases came from people either trying to forge a different person's signature, or by attempting to vote twice.

Before the pandemic, 5 states had voting by mail as the sole mechanism for voting: Oregon, Hawaii, Colorado, Washington, and Utah.[10] In these states, updated electronic voter registration rosters were used to send a single ballot to a single voter. In states that allow either in-person or mail-in/absentee voting, engaging in one option prevents the ability of a voter to use the other option as well. This ensures that each person could only cast a single ballot. Electronic rosters are consistently updated throughout the election process to determine the status of each voter's ballot, including whether one had been cast and by which method.[11]

To ensure that each mail-in/absentee ballot was cast by eligible voters on the voter registry, states use a variety of different processes. The most common is the signing of a voter affidavit assuring that the person submitting the ballot is who the ballot was addressed to. These signatures are checked with registration polls to ensure

[9] The Editorial Board, "The 2020 Election Won't Look like Any We've Seen Before," *The New York Times*, March 21, 2020, https://www.nytimes.com/2020/03/21/opinion/sunday/coronavirus-vote-mail.html.
[10] Lee, Michelle Ye Hee. "What's the Difference Between Absentee and Mail-In Voting?" Washington Post. Washington Post, August 18, 2020. https://www.washingtonpost.com/politics/2020/08/18/whats-difference-between-absentee-mail-in-voting/.
[11] "Electronic Poll Books | e-Poll Books." National Conference of State Legislatures, October 25, 2019. https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

they match before moving on to tabulation. Some states, such as California, Colorado, and Florida, ensure security through distinct, trackable barcodes or tally marks on each ballot that uniquely match to a single voter.[12] In this manner, one person cannot request and cast two separate mail-in ballots.

In most states that engage in mail-in/absentee voting, and in 46 states overall, voters can request and cast "provisional ballots."[13] The laws defining the eligibility of provisional ballots differ from state to state, but provisional ballots are typically used to allow citizens to cast ballots even if their voter eligibility is in question. The motivation behind provisional ballots is that a voter's eligibility or identity may not be guaranteed based on voter registration status. For instance, a voter might be trying to vote in the state they are registered in but not the correct district, or their registration information had not yet been updated. Until voter eligibility is ensured, provisional ballots are not counted towards election results. Thus, the voter must verify their registration in that district before their vote is tallied. Provisional ballots are a strong security check that still guarantees the principles of democratic elections, as they allow all people to vote without affecting the final tally until the voter proves their eligibility.

Once the paper ballots have been received and verified, they are finally counted. Voting machines tabulate mail-in ballots in largely the same manner as ballots cast at polling sites. The security of such voting machines will be discussed in Chapter 3. However, it is crucial to note that the security of casting and counting a ballot by mail is not inherently riskier than a ballot cast in-person. As far as current sampling can prove,

[12] Danetz, Lisa. "Mail Ballot Security Features: A Primer." The Brennan Center for Justice, October 16, 2020. https://www.brennancenter.org/our-work/research-reports/mail-ballot-security-features-primer.
[13] "Provisional Ballots." National Conference of State Legislatures, September 17, 2020. https://www.ncsl.org/research/elections-and-campaigns/provisional-ballots.aspx.

mail-in fraud happens at an infinitesimally small rate. As mentioned previously, in Oregon this rate has been about a dozen cases out of over 100 million ballots spanning two decades of voters.[14]

Voting In-Person

Until recently, filling out and/or turning in a ballot at physical polling centers was the traditional and most common method of voting. Voting in-person typically entails showing up at a polling center and requesting a ballot. Typically, this happens on election day, which is always on the Tuesday occurring from November 2nd to November 8th for federal elections. However, some states, such as Alabama, Maine, and many others, designate early voting periods where voters can cast ballots in-person in the weeks leading up to the election if they are unable to vote on election day itself. Once at a polling center, voters' names are checked against either physical or electronic pollbooks to ensure that the voter is registered and eligible in that district. In some states or districts this requires strict proof of identification, such as with driver's licenses or passports. In other states signatures are used. From here, states vary regarding how the voter casts their choice. Many jurisdictions allow the voter to fill out a physical ballot with a pen that is then submitted for later tabulation by machines. Other jurisdictions utilize some form of voting machine to designate a voter's selections. Such machines will be described in Chapter 3.

The potential issues with in-person voting are mainly the security risks inherent in many of the voting machines. Recently, however, there has been a growing attack

[14] Weiser, Wendy R, and Harold Ekeh. "The False Narrative of Vote-by-Mail Fraud." The Brennan Center, April 10, 2020. https://www.brennancenter.org/our-work/analysis-opinion/false-narrative-vote-mail-fraud.

against voters themselves committing alleged voter fraud throughout the nation. The largest and most controversial discussions have revolved around alleged "voter identification fraud," wherein a person illegally casts a ballot while pretending to be someone else. The imitated person could be either alive or dead, and identification fraud can happen either at polling centers or through mail-in ballots. If real, voter identification fraud would have the result of allowing someone to cast multiple ballots for a single candidate, potentially altering the outcome of close elections. To prevent such voter fraud from occurring, 36 states currently require proof of identification beyond a signature at polling centers to vote.[15] The exact laws vary from state to state, with the largest discrepancy being the types of identification accepted. Current debates on identification fraud question whether such laws are necessary. Advocates for the laws say that they make elections more legitimate, and opposers believe they are a discriminatory attempt to disenfranchise legitimate voters by making it more difficult to vote.[16]

Early research supports the latter opinion: that most of these laws have costs that vastly outweigh their benefits. The Brennan Center for Justice shows that the incident rates of identification fraud are between 0.0003% and 0.0025%.[17] This would mean that the average American has a higher likelihood of being struck by lightning than successfully impersonating someone else at the polls. Another study, conducted by the Republican National Lawyers Association (RNLA), found that, from 2000-2010, in

[15] "Voter Identification Requirements." National Conference of State Legislatures. National Conference of State Legislatures, August 25, 2020. https://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx.
[16] Newkirk, Vann R. "How Voter ID Laws Discriminate." The Atlantic, February 18, 2017. https://www.theatlantic.com/politics/archive/2017/02/how-voter-id-laws-discriminate-study/517218/.
[17] Levitt, Justin. Rep. *The Truth About Voter Fraud*. New York City, NY: Brennan Center For Justice, 2007.

over 20 states there were 2 or fewer convictions of voter identification fraud.[18] The state with the highest conviction number, Florida, had just 17 spread over the entire decade. Such data shows that, though voter identification fraud may sometimes occur, the perpetrators are largely unsuccessful, making paranoia surrounding the issue a case of smoke without fire. The few credible cases of voter identification fraud are irregularities in the overall electoral process, and far from the norm. The alteration of just a handful of votes over a decade long period with hundreds of millions of ballots cast is not enough data to suggest wide-scale voter fraud.

[18] Hines, Debbie. "New Republican Data Shows No Need For Voter ID Laws." Huffington Post, February 11, 2012. https://www.huffpost.com/entry/voter-fraud-statistics_b_1139085.

Chapter 3: Voting Machines

Introduction

Despite the diversity in voting laws among U.S. states, the core technology used throughout the United States remains largely consistent. The reason for this is because the market for voting machines is largely dominated by just 3 vendors: Election Systems & Software, the largest by a substantial margin, Dominion Voting Systems, and Hart InterCivic.[19] Although each state utilizes different combinations of technology, a few common machines produced by the 3 major vendors represent almost the entirety of American voters. Throughout this chapter, I will be looking at each of these voting technologies in detail to explain the breadth of their use and how they work. I will use this information to detail the security risks inherent in each of these machines. Recommendations for eliminating these risks will be provided in Chapter 5.

Pollbooks and E-Pollbooks

Pollbooks come in either an electronic or physical form and form the basis for verifying voter eligibility. At their core, pollbooks are collections of voter data information used to help citizens register to vote, cast ballots, and verify identities. Pollbooks are not used to tally vote counts or hold ballot information, but often reflect the voting status of registered citizens. Pollbooks are essential to checking that a person is registered to vote and has not already cast a ballot in the election. They are often used at physical polling centers during check-in and are utilized in mail-in/absentee voting to

[19] Fessler, Pam, and Johnny Kauffman. "Trips To Vegas And Chocolate-Covered Pretzels: Election Vendors Come Under Scrutiny." National Public Radio, May 2, 2019. https://www.npr.org/2019/05/02/718270183/trips-to-vegas-and-chocolate-covered-pretzels-election-vendors-come-under-scruti.

decide where and who ballots need to be sent to. For a state like Oregon, where all voting is done by mail, pollbooks are used to send ballots to every legally registered voter. For states where you can vote in-person or also at a physical poll center, the pollbook is used to make sure the voter only uses one of the provided mechanisms.[20]

Physical pollbooks are paper books containing a list of eligible voters in each district.[21] They are largely secure insofar that the physical book can only be accessed by election officials. The real concern with physical pollbooks comes in their electronic form, e-pollbooks, which tend to produce the physical copy. E-pollbooks are incredibly similar to their physical counterpart, however they are connected to an online voter registry containing all the aforementioned voter information. Such electronic databases are now utilized across the country in the form of laptops and tablets as states have continued to modernize their electoral processes over the last few decades. As of October 2019, according to the National Conference of State Legislatures (NCSL), e-pollbooks have been authorized by statute or have been used without explicit authorization to verify voters on election day in at least 41 states and D.C..[22] There are many benefits to using e-pollbooks that have contributed to their growing popularity. E-pollbooks provide real-time updates of voter history, ensuring that people cannot cast two or more ballots. Additionally, they can scan ID cards to pull up voter data, produce turnout numbers, can register voters on the spot, and allow poll workers to redirect voters to their correct districts, among other uses.

[20] "Electronic Poll Books | e-Poll Books." National Conference of State Legislatures, October 25, 2019. https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.
[21] Ibid.
[22] Ibid.

While e-pollbooks simplify and speed up the electoral process, there are inherent security risks involved with being constantly connected the internet. Cyberattacks could intercept internet signals fired off by the e-pollbook, allowing attackers to manipulate or delete voter data as well as block the transmission of identification verification practices. As will be discussed throughout Chapter 4, hackers have shown they are capable of breaking into virtual voter registries to manipulate or steal private voter information. Additionally, most states are not prepared in the event of a cyber-attack that causes the e-pollbooks to shut down entirely. If physical back-ups are not present, such attacks would stall or prevent voters from being able to cast their ballots as their information would be impossible to verify. States must take the risk of cyber-attacks into account when purchasing new e-book systems and when training poll workers to use such technologies.[23]

Ballot Marking Device (BMD)

Ballot marking devices (BMDs) are found in physical polling centers and are used to fill out paper ballots for the voter. Since lever-mechanisms are rarely used anymore following the events of the 2000 election, modern BMDs typically work through a touchscreen interface which voters interact with to select their candidates. After the voter inputs their choices, the machine prints out a paper card which the voter can check before submitting the ballot for later tabulation. BMDs are specifically designed with several services meant to assist disabled and elderly people in the voting process. Such machines rose to prominence following the Help America Vote Act of

[23] National Academies of Sciences, Engineering, and Medicine 2018. Securing the Vote: Protecting American Democracy. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.

2002, which mandated that each precinct must contain at least one accessible voting machine for disabled citizens.[24] BMDs are used throughout the nation, and most states that utilize BMDs have expanded their use such that many non-disabled or elderly people vote on them as well.

Ballot marking devices have many strengths that make them popular nationwide. Regarding security benefits, BMDs are not typically connected to the internet or any other network while voters are interacting with them, limiting the risk of remote hacking. Additionally, BMDs tend to allow voters to double-check their ballots after entering their selections and before turning the ballot in for tabulation. However, there are still fundamental technological issues surrounding BMDs that can slow down the voting process or introduce errors. Just as with all hardware tools, BMDs are entirely reliant on the software within them. Ballots need to be encoded into the system of BMDs for voters to be able to make their selections on the touch screen. Bugs resulting from the implementation of a ballot in the BMD's system can have massive ramifications on the voter's ability to vote for what/whom they intend.

Furthermore, while allowing voters to check the paper receipt from the BMD realizes the idea of software independence and reflects the necessity of a paper trail, the security of BMD systems is entirely reliant on how reliably voters check for, and correct, ballot errors. If errors are consistently caught and corrected, then BMDs are one of the most secure voting machines utilized. However, there is a growing concern that voters tend to skip the process of review. Without consistent reviewing of ballots by voters, BMDs could introduce bugs into many voter's ballots that go unnoticed for

[24] US House of Representatives Committee on House Administration, and Matt Blaze. Document, 2020 Election Security - Perspectives from Voting System Vendors and Experts § (2020).

extended periods of time.[25] This concern was tested in a study conducted by the University of Michigan Harker School.

The study aimed to uncover how often voters noticed errors in the ballots produced by BMD systems. In the study, 241 candidates were asked to cast a vote on a BMD that was intentionally coded to introduce specific errors on their ballots.[26] They then monitored how many voters checked their ballots and how many caught the error. To simulate the diversity of polling centers and poll workers that exist, they gave differing instructions to each candidate. The instructions ranged from no guidance following the voter receiving their paper ballot to asking each person individually if they had checked their ballot before turning them in. When no guidance was provided, only 39.7% of participants reviewed their ballot at all, and only 6.6% noticed an error and reported it to the poll workers.[27] Many participants could not remember who/what they had voted for just seconds earlier. When intervention by poll workers occurred, 64.3% of voters reviewed their ballot and 27.8% reported the error to the poll workers. This study shows that if BMDs are running with errors, the chance that these errors are caught and reported by voters is very low. Thus, it is crucial that poll workers not only encourage all voters to check their ballots, but also have the capability to probe BMDs for accuracy consistently. During election cycles where voters are consistently using the BMD machines, this can be done through manual tests on the BMDs throughout the day.

---

[25] Appel, Andrew W., Richard A. DeMillo, and Philip B. Stark. "Ballot-marking devices cannot ensure the will of the voters." Election Law Journal: Rules, Politics, and Policy 19, no. 3 (2020): 432-450.
[26] Bernhard, Matthew, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and Alex Haldermann. “Can Voters Detect Malicious Manipulation of Ballot Marking Devices?,” University of Michigan, n.d.
[27] Ibid.

Optical Scan Ballot Readers

Optical scan ballot readers are machines that take in physical ballots and keeps a running tally of voter choices for each selection. The machine stores the tally on removable memory devices that are directly connected to the system. Optical scan ballot readers are used on ballots collected through voter-marked ballots at polling centers, ballots received from absentee/vote-by-mail systems, or ballots produced by BMDs. After counting a ballot, the optical scan ballot reader typically locks away the voter's original ballot in a mechanically secured box connected to the machine. While this guarantees security for physical ballots, it also means that the voter typically does not have access to their ballot after being put through the machine. Although optical scan ballot readers preserve a reliable paper trail, voters cannot fix errors or change their selections after insertion into the machine.

The primary motivation for optical scan ballot readers is that they do not manipulate the voter's original ballot, they simply tally the results of voter's choices. Thus, they ensure software independence by keeping a verifiable paper trail through the preservation of the original ballots. Additionally, errors will only appear in tabulation rather than actually incorrectly marking a ballot for a voter. As such, so long as the voter ensures that their ballot selections are correct before submitting them, the work of optical scan ballot readers can be easily checked through human audits. These advantages have led to such machines gaining popularity throughout the nation. According to the Pew Research Center in 2016, 47% of voters lived in areas that use

optical scan ballot readers as the primary method to count votes.[28] An additional 19% of voters live in precincts that use optical scan ballot readers in conjunction with other tabulation machines.

While optical scan ballot readers have many advantages, case studies highlight the potential risks inherent in such machines. In one case, in the wake of a contentious 2008 Senate race in Minnesota, the state released 6,737 anonymous optically scanned ballot images to the public.[29] These images represent the scan collected by the voting machine, as well as the result that each ballot produced. While the ballots were used on 2008 machines, the core problems and security risks remain the same. One of the most prevalent risks identified was undetected failures in the reading of the voter's ballots. Based almost entirely on how a user filled in their ballot bubbles, optical voting machines were shown to misread the voter's selection by selecting an incorrect candidate, cancelling a box that a voter intended to vote for, or by not considering a vote altogether. The machines would only recognize clearly defined bubbles while not accounting for human errors in otherwise valid ballots. Thus, a voter could believe they filled out a ballot correctly while an optical scanner did not count their choice towards the results tally.

The study found additional risks dependent on the layout of the ballot itself. The images studied showed that certain areas of the ballot misread more often than others, showing that a candidate's location on the ballot might have large technological

[28] Desilver, Drew. "On Election Day, Most Voters Use Electronic or Optical Scan Ballots." Pew Research Center, November 8, 2016. https://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/.
[29] Lopresti, Daniel, George Nagy, and Elisa Barney Smith. "Document Analysis Issues in Reading Optical Scan Ballots." In *Proceedings of the 9th IAPR International Workshop on Document Analysis Systems*, 105–12. Boston, MA: Association for Computing Machinery, 2010.

implications on how many votes they received.[30] Though the software can, and has, been improved regarding how ballots are read, there is still a risk that a vote may be miscounted or not counted at all. With optical scan ballot readers, the voter typically has no way to ensure that their ballot was counted as intended. There may have been a disconnect between which candidate the voter chose on the ballot and which one the optical scanner chose for the voter. While this can be double checked through the auditing of the intact paper trail produced, most precincts only run such audits in the case of close elections. When the election result seems clear, most jurisdictions will rely entirely on the machine's result. This runs the risk of counting out certain voters entirely. While optical scanners may work well when user error is not introduced, they fall short when voters make errors, such as using non-conforming marking styles (See Figure 1) or attempting to cancel a vote (See Figure 2).

The study shows that optical scan ballot readers both fail and excel at ensuring the idea of software independence. While a human component still exists through the physical ballot that is inserted into the optical scanner, the machines do not display critical reasoning in accounting for human errors. Optical scanners fall short of software independence as the scanning happens during the tabulation phase at the end of the electoral process, after the voter no longer has access to their ballots. Thus, there must be some degree of human reasoning when tabulating votes so that all votes are counted accurately and as intended. This human component could take form through consistent risk-limiting audits after each election, which will be described in Chapter 5.

[30] Ibid.

Direct Recording Electronic (DRE) Voting Machine

Direct recording electronic voting machines (DREs) are the epitome of voting machines in the digital age. To modernize electoral processes, DREs flooded onto the scene within the last two decades. The typical DRE systems are equipped with a touch screen like a BMD wherein voters make their choices. The base ballot that is presented to the voter is stored internally on the device on removable memory cards and programmed into the system. The largest difference between a BMD and a DRE is that once the voter makes their selections on a DRE they are tallied and stored on other removable memory cards rather than a physical paper ballot. In this manner, the voting process is entirely electronic. While some newer DREs produce a paper trail, a large amount of DREs in use today do not.

Regarding paperless DRE systems, the Brennan Center found as late as 2019 that 12 states still used paperless DREs as the primary polling device throughout many of their counties and towns. Of these 12, 4 states (Delaware, Georgia, Louisiana, and South Carolina) use paperless DREs as the primary system throughout the entire state.[31] Such widespread use has led to 28% of Americans living in DRE-only jurisdictions as of 2016. An additional 19% live in jurisdictions that use a combination of DRE and optical scan ballot readers.[32]

The prevalence of paperless DRE systems is troubling, as experts have shown time and again that they are one of the most insecure voting systems. Due to their

[31] Norden, Lawrence, and Andrea Córdova McCadney. "Voting Machines at Risk: Where We Stand Today." Brennan Center. Brennan Center for Justice, March 5, 2019. https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-where-we-stand-today.
[32] Desilver, Drew. "On Election Day, Most Voters Use Electronic or Optical Scan Ballots." Pew Research Center, November 8, 2016. https://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/.

almost entirely digital nature, paperless DREs are susceptible to attacks that are not traditionally prevalent in machines that work with physical ballots. These attacks can take form in multiple ways, such as by deleting vote tallies stored in a DREs digital media or altering final result tabulations on the removable memory card to change votes. Through external interface ports, hackers can access data files stored on the machine's internal and/or removable memory. Additionally, the ballots that voters use on these machines are themselves encoded in the machine. Since the ballots are stored on digital memory, tampering could be done to change the format or selections on the actual ballot itself.[33]

The potential security risks of DRE systems do not end there. Hackers can also access electronic log files stored within the DRE to disrupt post-election audits and can even disable security software that detects when a machine has been tampered with. The hacker could upload a corrupt software that looks identical to the original but is maliciously altered to disturb the results. Even if the hacker did not replace the software, most DREs still have flawed software that allow hackers to exploit vulnerabilities that already exist.

A 2007 study in California and Ohio showed that any of these exploitations could be done by a single person with no more access than the typical poll worker or voter.[34] The study showcases that voters have more private access to DRE systems than any other voting machine. With extended access, a knowledgeable hacker could override passwords to disrupt the machine digitally or interfere with the physical

[33] US House of Representatives Committee on House Administration, and Matt Blaze. Document, 2020 Election Security - Perspectives from Voting System Vendors and Experts § (2020).
[34] McDaniel, P., Matt Blaze and G. Vigna. "EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing." (2007).

removable media of the machine. Though the study is over a decade old, many states still use the same machines be it due to cost of replacement or other reasoning. Thus, DRE systems are not only ill-equipped to deal with potential security flaws which can lead to inaccurate election results, but DREs also do not allow for secure post-election audits to occur. With paperless DREs, there is no way to ensure the original intent of voters.

Chapter 4: Foreign Interference and Hacking Methods

Introduction

The previous sections have outlined many security risks that are present throughout the ballot collection and tabulation process in every single state. Such explanations show that America's elections come with inherent risks as they continue to adapt to a technologically complex world. Though these risks could be exploited by domestic groups or individuals, it is much more likely that American elections will be hacked by some foreign body. The reason for this is because most domestic occurrences of exploiting vulnerabilities in voting technology have the goal of changing the number of votes for a given candidate. This ideology is akin to the older idea of stuffing ballot boxes to ensure victories. While such an attack may have massive implications for the future of the United States, they would have to occur on a large scale and thus are much less likely to occur and much easier to catch through post-election audits.

A very real threat comes in the form of foreign interference, largely by exploiting technological vulnerabilities through cyberattacks. Foreign entities do not necessarily need to change the outcome of an entire election to achieve their goals. Rather, their goals tend to be centered around destabilizing the democratic institutions of the United States by planting a seed of doubt in the minds of American citizens. Such doubt can be achieved simply by calling the results into question by asserting their presence at any point throughout an election. This is a much easier goal to achieve than overturning an entire election through tabulation manipulation.

The goals described above is exactly what Russia attempted to achieve when interfering with the federal election of 2016.[35] It is unlikely that they changed a single vote, but rather they simply asserted that they had the capability to do so through asserting their presence in private voter databases and machines. This represents a massive security breach that could happen at any time if the United States' election infrastructure is not prepared, giving the foreign body access to millions of copies of private voter data and the potential to change ballots and steal secure voter data. Dissecting the 2016 election and the threat of foreign interference will be the topic of this section.

What We Know From 2016 to Now

In conducting research about the 2016 Federal Election, the most important document is the Senate's Select Committee on Intelligence's report on *Russian Active Measures Campaigns and Interference in the 2016 Presidential Election*. Though the report comes chock full of redactions, there is still a wealth of information on how foreign states, namely Russia, interfered with the 2016 election. However, the story does not start in 2016. Rather, the Committee found that "The Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure at the state and local level."[36] This means that Russian actors have been interfering with election systems since at least the 2014 midterm elections, through the 2016 election, and likely continuing to the modern day.

[35] United States Senate Select Committee on Intelligence. Report, 1 Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views §. 116-290 (116AD).
[36] Ibid.

As mentioned previously, Russian interference likely has not involved changing actual vote tallies, the Senate seems very certain that results were not changed. Rather, the goal of foreign interference in 2016 was to influence the general electorate into making specific candidate choices, as well as to show that they had the capacity to exploit systems further should they want to.

Though Russia has been exerting efforts to interfere with federal elections since at least 2014, palpable interference gained momentum in 2016 just before the Democratic National Convention (DNC).[37] The Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), Russia's military intelligence agency, hacked into DNC servers, as well as the email of the Chairman of Secretary Hillary Clinton's campaign, John Podesta. The goal of the hack being to leak their private emails to the public through WikiLeaks, a website where people often anonymously publish classified information.[38] The emails were likely hacked through a cyber-attack technique called "spear-phishing." A spear-phishing attack entails sending emails that appear legitimate but contain links that, when pressed, contain vicious malware (computer viruses) that give the attackers prolonged access to the user's system.[39] In this case, that access was used to hack into email servers and steal private information. Discussions surrounding the private emails, largely based around their classified contents, would go on to dominate the DNC news cycle as well as cast a

[37] Lamond, James, and Jeremy Venook. "Blunting Foreign Interference Efforts by Learning the Lessons of the Past." Center for American Progress, September 2, 2020. https://www.americanprogress.org/issues/security/reports/2020/09/02/489865/blunting-foreign-interference-efforts-learning-lessons-past/.
[38] Ibid.
[39] Caputo, Deanna D, Shari Lawrence Pfleeger, Jesse D Freeman, and M Eric Johnson. "Going Spear Phishing: Exploring Embedded Training and Awareness." *IEEE Security & Privacy* 12, no. 1 (August 26, 2013): 28–38. https://doi.org/10.1109/MSP.2013.106.

shadow over Secretary Clinton's entire campaign. Other information was stolen from both Republican and Democratic leaders, but such information was not leaked, and it remains a mystery what was done with this data.

While such instances reflect an obvious concern for our nation's cybersecurity infrastructures, the real danger comes with foreign actors attempting to delegitimize the actual voting process. Interference became apparent in July 2016 when the state of Illinois reported that there was unrecognized network activity on the Board of Electors' Voter Registry. The attack resulted in the exfiltration of voter data, meaning an unauthorized transfer of voter data to the attacker.[40] The FBI then issued a FLASH alert on August 18, 2016, to every state to check if certain suspect IP addresses identified from Illinois had been seen on any other state's voting systems. An IP address is an "internet protocol" address that uniquely identifies any device on the internet as well as that device's location. By tracking common IP addresses, the FBI hoped to track where the attacks were coming from. From this first FLASH alert, the FBI found that it was apparent that election infrastructure and voter databases had been probed by Russian IP addresses in at least 21 different states.[41] A second FLASH alert, conducted in October 2016, concluded that it was likely that all 50 states had been probed. While the probing activity differed from state to state, the common aspects of election infrastructure that were interfered with was voter identification information from private voter databases,

[40] United States Senate Select Committee on Intelligence. Report, 1 Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views §. 116-290 (116AD).
[41] Ibid.

election system software for collecting and tabulating ballots, election-related web pages, and election service companies.

The Senate Committee on Intelligence and the US Department of Homeland Security (DHS) compared tactics, techniques, and procedures (TTPs) used by the foreign actors to previously observed Russian TTPs to conclude that the Russians were in fact the ones probing election infrastructures.[42] The DHS Intelligence Assessment on this issue reported that the actors were targeting election infrastructure for a myriad of purposes. Among these were to cause disruptive effects in American elections, undermine the confidence of the public in respect to the final tally, and to steal sensitive voter data. The first two points suggest that foreign actors are attempting to delegitimize American elections in the eyes of the public with the goal of having extremely disruptive effects on American democracy. However, it is the third point that represents the largest danger to election security, as stealing voter data requires direct access to voter registration databases, meaning foreign actors in voter registries could cause a lot more harm than just stealing data.

The report by the Senate's Committee on Intelligence shows that, by the end of 2018, Russia had accessed up to 200,000 voter registration records in Illinois.[43] While data about the other 49 states is not publicly available, the implications of the case in Illinois causes reasons to worry. Having access to voter registration records not only gives away the personal data of every individual voter, but also gives them the ability to change or delete voter data from the system entirely. While the Committee does not believe this occurred in 2016, it shows that foreign actors, specifically the Russians in

[42] Ibid.
[43] Ibid.

this case, had the capability to massively alter both current and future elections if they had the goal of altering the databases.

Foreign Interference on Election Websites

The attacks used to access voter databases may take several forms. An extremely common and basic way employs the aforementioned spear-phishing method, wherein poll workers or others with direct access to voter registries are sent virus-ridden emails. However, spear-phishing is not a particularly advanced attack and is easy to avoid if those vulnerable of being hacked know what to look out for. There are many other types of database exploitation techniques that can also give complete access to online voter databases with the additional threat of being much harder to defend against. The best case to examine here would be Vermont's Online Voter Registration Application (OVRA), which the DHS reported that cybersecurity officials detected multiple attempts to access on August 24, 2018.[44] While the attacker here has not been disclosed, the TTPs have been. While, in this instance, the attacks were only conducted on one website in Vermont, the TTPs employed are commonplace among cybersecurity attacks on both election infrastructure and traditional websites.

One of the attacks on the OVRA came in the form of cross site scripting (XSS). XSS is a form of "injection attack," meaning some attacker provides malicious input into a program that gets processed and then executed. While there are many different types of XSS, attacks typically involve the injection of malicious scripts into safe websites that ask for user input where said input is not validated or encoded. The term "script" in this context refers to a series of commands that are given to a program.

[44] Ibid.

Scripts are often used to automate processes but can also be used maliciously to run unauthorized commands on otherwise secure browsers. With XSS, the scripts are given in the form of user input, such as when asking for a login name. Because the website believes the script is simply user input, the website thinks that the script is trustworthy and, as such, runs the malicious commands. The goal of a XSS attack is to attack the users of the website, often by redirecting them to insecure website locations where the attacker can steal personal data, such as credit card data, social security information, or passwords off their computers.[45]

The OVRA also received seven Structured Query Language (SQL) injection attempts. SQL by itself is a programming language commonly used to access and manage database systems. SQL injection occurs when an attacker providing user input provides a SQL statement that will be read and executed by a database. The difference between SQL injection and XSS is that the goal of SQL injection is to attack the website's database itself. XSS attempts to steal secure data from the user, whereas SQL injection attempts to access databases.[46] The result of SQL injections could be the deletion or manipulation of otherwise secure voter databases, or unauthorized access to data stored within the database. If databases are not protected, attackers could gain access to all the information stored within a voter registration database through simple SQL commands. Luckily, the OVRA was able to fend off the seven attempts, but it is unclear how many voter databases in the country are prepared to do so.

[45] Shalini, S., and S. Usha. "Prevention Of cross-site scripting attacks (XSS) on web applications in the client side." International Journal of Computer Science Issues (IJCSI) 8, no. 4 (2011): 650.
[46] Martin, Michael C., and Monica S. Lam. "Automatic Generation of XSS and SQL Injection Attacks with Goal-Directed Model Checking." In USENIX Security symposium, pp. 31-44. 2008.

The final type of attack that the OVRA received was a single attempted Denial of Service (DoS) attack, which also failed. DoS attacks do not attempt to steal data, rather their goal is to take down websites/services so that legitimate users are unable to use them for extended periods of time. DoS attacks are carried out by an attacker essentially overloading a service with internet requests. The attacker directs a constant stream of attempts over time such that the website either fails to respond or crashes entirely. While DoS attacks do not necessarily disturb data on their own, they prevent users of a service from being able to access it. Additionally, DoS attacks are often used to make a service vulnerable to future attacks such as those outlined above. In the context of election infrastructure, a successful DoS attack on a website such as the OVRA would prevent users from being able to register to vote, identify themselves at polling stations, or check the status of their ballots. While the service is down and vulnerable, the hacker could use the DoS attack in conjunction with other hacking methods to steal secure voter data. Again, the DoS attack on the OVRA was prevented, but the existence of such attacks reflects another security concern nationwide and the need for contingency plans.

Foreign Interference Implications on Voting Machines

Up to this point the discussion of foreign interference has revolved around voter registration databases and voting websites. However, such attacks in turn reveal imperfections about the voting machines described throughout Chapter 3. The Senate's Committee on Intelligence found that potential hackers could gain remote access to voting machines used in 41 states, hacking systems used by around 50% of American

voters.[47] While offline machines tend to be protected from remote hacking, many machines, such as DREs and BMDs, connect to a local network at some point throughout the election process, often to download software containing ballot layouts onto the machine.

For example, while best practices dictate that DRE systems should be disconnected from the internet, each machine needs to be programmed before the date of an election to put the correct ballot in place. The programming is often done by connecting the machine to a local network or by downloading software off some form of removable media, such as a thumb drive. If the computer responsible for producing and releasing the program is compromised, then every single system that utilizes the same code will also be compromised. Additionally, not all precincts follow best practices, meaning many DRE systems remain connected to local networks indefinitely. While connected to local networks, hackers could access any number of machines in a polling center.

While remote hacking reveals a large concern with current voting machines, many of the machines used throughout the country can be easily hacked from within a polling place with no greater access than any typical voter would have. This is evidenced through the DEF CON Conference's *Voting Machine Hacking Village* ("Voting Village"). DEF CON is an annual convention based around cybersecurity and hacking. Within the Voting Village, hackers of all different levels of expertise come into contact with a myriad of voting machines, including DREs, optical scan ballot

[47] United States Senate Select Committee on Intelligence. Report, 1 Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views §. 116-290 (116AD).

readers, BMDs, and electronic pollbooks.[48] Each machine is authorized for use in at least one jurisdiction, and hackers attending the conference are encouraged to attempt to break into the machines through the access level any typical voter would have. The results of this experiment are alarming. Though the hackers have very limited expertise in voting machines specifically, the hackers managed to exploit vulnerabilities in every machine over the course of two days. Matt Blaze, a computer science researcher and organizer of the Voting Village, stated in a testimony to Congress that:

> Depending on the individual model of machine, participants have found ways to load malicious software, gain access to administrator passwords, compromise recorded votes and audit logs, or cause equipment to fail. In most cases, these attacks could be carried out from the ordinary interfaces that are exposed to voters and precinct poll workers.[49]

Through the Voting Village, Blaze shows us that existing voting machines employed throughout the country are entirely fallible. The hacking attempts were not conducted by voting machine experts in an unrealistic lab setting. Rather, the machines were exploited in real-time settings by people with varying levels of expertise over the course of just a few days. Such interference would allow hackers to entirely disable the machines, change vote tallies, and generally produce enough damage to call the results of an election into question. Although local hacking of this variety has largely not occurred and would be incredibly difficult to carry out on a national scale, it could still influence local elections and call results from certain states into question in larger elections. We have seen from previous presidential elections the significance of even just a single state's vote count being called into question.

---

[48] US House of Representatives Committee on House Administration, and Matt Blaze. Document, 2020 Election Security - Perspectives from Voting System Vendors and Experts § (2020).
[49] Ibid.

Chapter 5: Recommendations

Introduction

The previous chapters described and assessed the risks of various voting methods, election infrastructures, and the implications and tactics of foreign actors. However, they have done little in the way of providing actual solutions to the prescribed problems. Recommendations are necessary because, as of 2017, the Department of Homeland Security has designated elections infrastructure as "critical infrastructure."[50] This means that matters of election security receive the top priority of the federal government. This designation denotes that improvements need to be made in every state regarding election security, and that the federal government will help enact changes through funding, oversight, and proposed legislation. With a keener eye on election infrastructure comes a need for direction in how to approach changes, as not every representative is an expert on voting systems. Throughout this section, recommendations will be made with the goal of enhancing the technological security of election infrastructure without restricting access to the ballot. The recommendations are not ordered by importance and will be divided between in-person/mail-in voting, voting machines, voter databases, and voting procedures.

[50] National Academies of Sciences, Engineering, and Medicine 2018. Securing the Vote: Protecting American Democracy. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.

Mail-In/Absentee Voting

All Precincts Must Provide Means for Mail-In/Absentee Voters to Check the Status of Their Ballots at Any Point in Time

To ensure that all ballots are counted as intended, states must ensure that any voting citizen who is voting by mail/absentee can check the status of their ballot at any point leading up to the election. Before casting a ballot, voters should be made aware that a ballot has been mailed to them. After submitting the mail-in ballot, voters should be able to check whether the ballot has been received and counted. This should be done through mail, email alerts, website portals, or mobile phone apps which only show the status of the ballot rather than any sensitive information or candidate choices. In this manner, voters are made readily aware of the status of their ballot without compromising secure data. A single response of "yes" or "no" regarding if a ballot has been received and/or counted would suffice.

There are 45 states that supported online ballot tracking throughout the entire state in the 2020 Presidential Election.[51] Of the 5 states that did not – Texas, Illinois, Mississippi, Missouri, and Wyoming – there are certain counties, such as Cook County in Illinois, that provide ballot tracking capabilities. Other states, such as Texas, provide ballot tracking only for military personnel.[52] While these are steps in the right direction, ballot tracking must be implemented statewide for all mail-in/absentee voters. Additionally, of the 45 states that provided ballot tracking services in the 2020

[51] Conklin, Audrey. "Was My Vote Counted? A State-by-State Guide to Tracking Your Absentee Ballot." Fox5Atlanta. Fox Broadcasting Company, November 3, 2020. https://www.fox5atlanta.com/news/was-my-vote-counted-a-state-by-state-guide-to-tracking-your-absentee-ballot.
[52] Ibid.

Presidential Election, voters often had to opt-in or visit various websites with their private information to check their ballots in many states. Voters should automatically be enlisted in ballot tracking programs when registering to vote. Finally, such ballot tracking services should be available for all elections at all levels of government rather than just for federal elections, as all votes in every election matter.

All Precincts Must Provide Means for Mail-In/Absentee Voters to Correct Ballot Errors

If there are detectable errors on the ballot, such as an unmatched signature, name, or address, voters must be made aware through the aforementioned ballot tracking service and there must be a system in place to allow them to prove their identification. According to the National Conference of State Legislatures, as of September 2020 there are 18 states that provide means for voters to correct ballot errors.[53] The laws vary greatly from state to state, with some states allowing ballot corrections only up to election day and others allowing for correction up to two weeks following an election. Oftentimes voters are not made aware of when their ballots are rejected, which is why this service would go hand-in-hand with the aforementioned ballot tracking technology.

Correcting ballot errors is not to say that voters should be able to change the selections they made. Rather, voters should be able to prove their identity and that they are eligible voters, thereby ensuring the validity of their selections. This is the same ideology as with provisional ballots, the only difference being that many mail-in voters are largely unaware of the status of their ballots. Provisional ballot casters know they

[53] "States That Permit Voters to Correct Signature Discrepancies." National Conference of State Legislatures, September 21, 2020. https://www.ncsl.org/research/elections-and-campaigns/vopp-table-15-states-that-permit-voters-to-correct-signature-discrepancies.aspx.

have to verify their eligibility for the ballot to be counted, whereas mail-in voters may submit a ballot they believe to be valid that ends up not being counted. The Pew Research Center shows that, in the 2016 election, more than 400,000 mail-in votes were not counted. The largest reason for this, coming out to approximately 28.3% of rejected absentee ballots, was because of non-matching signatures.[54] While it is good that security measures reject such errors rather than include them during tabulation, voters who voted legally should be able to prove their identification and have their ballot count. With such systems in place, greater scrutiny could be applied towards security measures when scanning ballots as there would be a system in place to verify each voter in question.

Voting Machines

Only Use Machines that Provide a Verifiable Paper Trail/Abandon Paperless DREs

All voting machines should be able to ensure software independence through their ability to produce a verifiable paper trail. Paper trails are important as they provide a safeguard against the possible corruption of a voter machine. When verifiable paper trails are utilized properly, all work done by voting machines can be double checked by a human hand. Should machines generally malfunction or get hacked to produce incorrect results, the original paper ballots would be able to be checked to detect alterations.

[54] Desilver, Drew. "Most Mail and Provisional Ballots Got Counted in Past U.S. Elections – but Many Did Not." Pew Research Center. Pew Research Center, November 10, 2020. https://www.pewresearch.org/fact-tank/2020/11/10/most-mail-and-provisional-ballots-got-counted-in-past-u-s-elections-but-many-did-not/.

Producing a verifiable paper trail means phasing out voting machines that do not adequately support paper ballots. As an example, paperless DRE systems do not come into contact with or produce a paper ballot at any point throughout the electoral process. Rather, voters input their selections into a programmable ballot displayed on a touch screen and the results are saved in the system's storage. As thus, such voting machines should be phased out of use and replaced with machines that allow results to be checked by humans.

Having a verifiable paper trail does not mean all voting machines must be phased out of the process entirely. On the contrary, paper ballots can be marked and counted by machines and still produce a reliable paper trail. Most BMDs already have this functionality, with some having the added bonus of allowing voters to check their selections before tabulation. Paperless DREs are the primary culprit in this discussion, as the entire voting process, from casting to tabulation, occurs within the memory device on the machine. Paperless DREs make it much more difficult to catch fraud. Additionally, if fraud were to occur, the original intent of the voters could be lost. There must be some physical receipt that matches each voter to their selections such that the receipts can later be examined in post-election audits.

All Voters Should Be Able and Encouraged to Check Physical Paper Receipts from Machines for Errors

To ensure that the paper trails produced by machines are accurate, machines that produce paper trails should allow the voters to check the paper receipts before submitting them to poll workers. This is akin to a voter double-checking their physical ballot before submission. Voting devices that mark ballots, such as BMDs, should

return at the minimum a copy of the paper receipt. Voters should be encouraged by poll workers at polling stations to check the results of the machines to ensure all machine results are what the voter intended.

The same should be done for machines that scan physical ballots, such as optical scan ballot readers. Many optical scan ballot readers lock the original ballot into a box without allowing the voter to see how it counted their ballot. While this ensures a paper trail, the machine should also output a separate physical receipt for the voter stating the voter's selections such that the voter can verify the results of the machine. If this is not possible, then the machine should show the result of the voter's choices on the touchscreen, manually making the voter verify their selections are accurate. If the scanning does not occur with the voter present, the outcome of the tabulation should be trackable on the aforementioned ballot tracker. With ballot tracking technology it is unwise to transmit the exact ballot, but systems could notify voters on whether or not the ballot was counted. To check tabulation, risk-limiting audits should be conducted by experts after each election. Risk-limiting audits will be discussed further below.

Voter Databases/Pollbooks

Election Officials Should Routinely Probe Voter Databases to Ensure Integrity

Election officials in every state must develop procedures for routinely checking online voter database systems. The 2016 general election and the 2018 hacking efforts on Vermont's voter registry emphasize the need for constant surveillance, especially in the months leading up to an election. There are several basic ways to probe voter databases to check for any sorts of tampering. The first is through checking the internet protocol (IP) addresses that come in and out of databases. As mentioned previously, IP

addresses are unique identifiers for all devices connected to the internet. Through cross-comparing IP addresses with other states and the DHS, precincts should be able to identify suspicious activity coming from inside and outside of the country. IP addresses that are constantly changing or are performing irregular amounts of activity in comparison to the average user are examples of where the system may be compromised.

Another way to check for irregularities is through monitoring spikes in database usage. If a hacker can gain administrative access to a database network through a user account, then the hacked user tends to attempt to give themselves heightened privileges which give them increased access to the system. If authorized users are performing an irregular number of functions and activities, especially if coming from unknown geographic locations, then that user may be hacked. Spikes in database usage can come from unauthorized or anonymous accounts as well. The aforementioned SQL injection cyberattack is an example of this, as the HTTP response to an injection attack will typically be much larger than a normal HTTP response. An HTTP response is between the server, such as a voter registry, and a client, such as a hacker.[55] They are the primary tool used on the internet to provide users with the information they request. Requesting a large amount of information entails a larger HTTP response, which can be tracked to suspicious behavior if large responses are irregular. The reason for this is because hackers tend to download large databases to get as much secure information as possible. This can take terabytes of data, which is much larger than a usual request. Election administrators should monitor the number of downloads and alterations coming from a database, as many of either could mean the system has been compromised.

[55] "HTTP Responses." IBM. International Business Machines, February 7, 2021. https://www.ibm.com/docs/en/cics-ts/5.3?topic=protocol-http-responses.

Finally, election administrators should monitor when databases go down and assess reasoning for as to why. Denial of service attacks (DoS) that aim to take functions offline are a common way that hackers can make an otherwise secure system vulnerable to future attacks. Such attacks tend to be designated by websites going down, slowed speeds, and general poor system performance. All of this data is trackable. In all cases where potential hacking may have occurred, the DHS should be notified immediately such that other states can check their databases for unusual activity as well. It is imperative the DHS is contacted immediately, as the case of 2016 shows that by the time the FBI got involved at least 21 states had been probed.[56]

Create Firewalls Between All Voting Processes and the Internet

The term "firewall" originally comes from the construction industry in reference to flame-proof barriers meant to limit or stop fires. In the world of computing, firewalls are a digital security device that filters internet requests coming in and out of a service. Their purpose is to stop suspicious activity from breaching some private service while still allowing access for authorized users. There can be many layers to a firewall, each protecting against different types of attacks. A large way this is accomplished is through the monitoring of HTTP requests. Anytime somebody does something on the internet, such as clicking on a webpage, an HTTP request is sent from the client computer to whatever server the user is attempting to access. If the request is accepted, the server will then send back an HTTP response containing the requested data.

[56] United States Senate Select Committee on Intelligence. Report, 1 Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views §. 116-290 (116AD).

Firewalls for voter database servers would live between the client and the server and filter the requests accepted from the client. A way many servers accomplish this is by managing the types of requests that the server will accept from different sources that try to access it. For example, firewalls could be configured to allow requests for credentialed users to view their own information, while simultaneously blocking requests where users try to manipulate their information or access other private records. In short firewalls could be configured to block certain types of HTTP requests which would lead to the alteration or destruction of databases. As a more discrete example, PUT requests are used to create/update resources and DELETE requests are used to remove resources. The GET request is used to request information. In the context of a voter registry, a firewall could block PUT/DELETE requests entirely unless authorized by a trusted user, such as an election administrator. While firewalls do not provide a completely impermeable defense against cyberattacks, they serve as a strong additional layer of security on top of other security measures.

Online Pollbooks Must Have Physical Backups

Due to the nature of online pollbooks, namely the fact that they are intertwined with internet networks, there must be physical backups. In the case that hackers, either foreign or domestic, can access databases, physical backups are necessary to preserve an accurate copy of currently registered voters. The motivation behind this recommendation is similar to the motivation behind verifiable paper trails for voting machines. Namely, there should be physical backups for all electronic services so that the electronic services can be verified. With two different modes of record keeping, constant comparisons between the digital and physical copies will ensure that neither

have been altered. Additionally, if online databases were to go down, physical backups allow for voting processes to continue at physical locations while precincts attempt to get the databases back online.

Voting Procedures

Discourage/Prevent Voters from Voting Through Online Formats

As technology continues to develop, there have been growing conversations about potentially allowing citizens to vote remotely from their own homes through the internet. While convenient, domestic cybersecurity technology is not nearly advanced enough to allow this to occur. If foreign actors can breach official government websites, then there is no question whether they could block or alter transmissions from remote devices on home internet connections. Currently, the only people that vote online are military personnel serving overseas and certain citizens abroad that are registered in states that allow it.

Even though a select few citizens already vote online, experts believe that what they are doing is incredibly insecure. An audit conducted by MIT found the Voatz app, the voting platform used by West Virginia and Oregon to facilitate ballot casting and collection to the few citizens that can vote online, to be dangerous to the integrity of elections. MIT researchers Michael Specter, James Koppel, and Daniel Weitzner wrote in the audit report that "Given the severity of failings discussed in this paper, the lack of transparency, the risks to voter privacy, and the trivial nature of the attacks, we suggest that any near-future plans to use this app for high-stakes elections be abandoned."[57]

[57] Newman, Lily Hay. "Voting App Flaws Could Have Let Hackers Manipulate Results." Wired. Condé Nast, February 13, 2020. https://www.wired.com/story/voatz-voting-app-security-flaws/.

Such strong words from leading experts shows that the technological capabilities of election infrastructure are not yet advanced and secure enough to prevent attacks, and as thus should be avoided in favor of paper-based methods. Due to the limited nature of online voting this insecurity has not posed a large issue thus far. However, efforts to expand online voting should not be undertaken until the platforms exemplify their ability to reject advanced cyberattacks.

Risk Limiting Audits Should be Used After Every Election

Risk limiting audits are a method of confirming election results based on statistics. The method is to review a random sample of physical paper ballots to determine that the outcome claimed by computers matches that of the verifiable paper trail.[58] This review is done entirely by humans and confirms or denies electoral results based on sampling a large number of ballots with a high statistical significance. Risk limiting audits are the reason behind software independence, as states must be able to verify machine results against a human hand. While many states conduct audits when elections are close, audits should be conducted after every Federal election regardless of the outcome. For local elections, audits should be done when the jurisdictions have the resources to do so. It is the best current way to verify an election's result by proving there has not been machine tampering.

In accordance with previous recommendations, states should only be purchasing and using voter equipment that allows for risk limiting audits to be conducted through a verifiable paper trail. As of February 2020, there only 3 states that require risk limiting

[58] Korte, Andrea. "AAAS' EPI Center Shares the Science of Election Security," Science Magazine. AAAS, June 28, 2019.

audits after elections by statute: Colorado, Virginia, and Rhode Island. There are 3 more states that have implemented statutory pilot programs to test the feasibility of such audits: Georgia, Indiana, and Nevada.[59] There are 6 more states that have begun to implement risk limiting audits in some form. This means that there are 38 states that are not prepared to perform audits when elections may be insecure. Such states are susceptible to election attacks as the results of their machines cannot be verified.

[59] "Risk-Limiting Audits." National Conference of State Legislatures, February 2, 2020. https://www.ncsl.org/research/elections-and-campaigns/risk-limiting-audits.aspx.

Conclusion

In conclusion, as the United States continues to adapt to an increasingly technological world comes increasing threats to election security. These risks do not come in the form of traditional voter fraud covered in the media, such as voter identification fraud. Rather, elections are most likely to be exploited through the technology used to facilitate the electoral process. Paperless voting machines, such as many types of DREs used throughout the nation, pose a major risk as they prevent the ability to accurately audit elections. In order for the collection of ballots to be secure, software independence needs to be maintained through verifiable paper trails and post-election audits. Regarding voter registries, the 2016 election showed that they are not fully capable of fending off attacks from foreign or domestic hackers. While the Department of Homeland Security has designated elections infrastructure as "critical infrastructure," further attention and efforts need to be made to increase cybersecurity.

Though there have been no signs of election results being changed, there has been evidence that foreign and domestic actors have had the capability to do so either through online voter registries or through voting machines. Therefore, it is essential that government actors begin, if they have not already, to implement the types of recommendations I made throughout this paper, as well as the recommendations of the countless professional experts in the field, in order to further guarantee the security of future elections at all levels. Elections must continue to be fair with each voter confidently knowing that the ballot they cast is counted equally and as intended. The only way to guarantee this fundamental democratic principle is by ensuring the technological security of American elections.

Appendixes

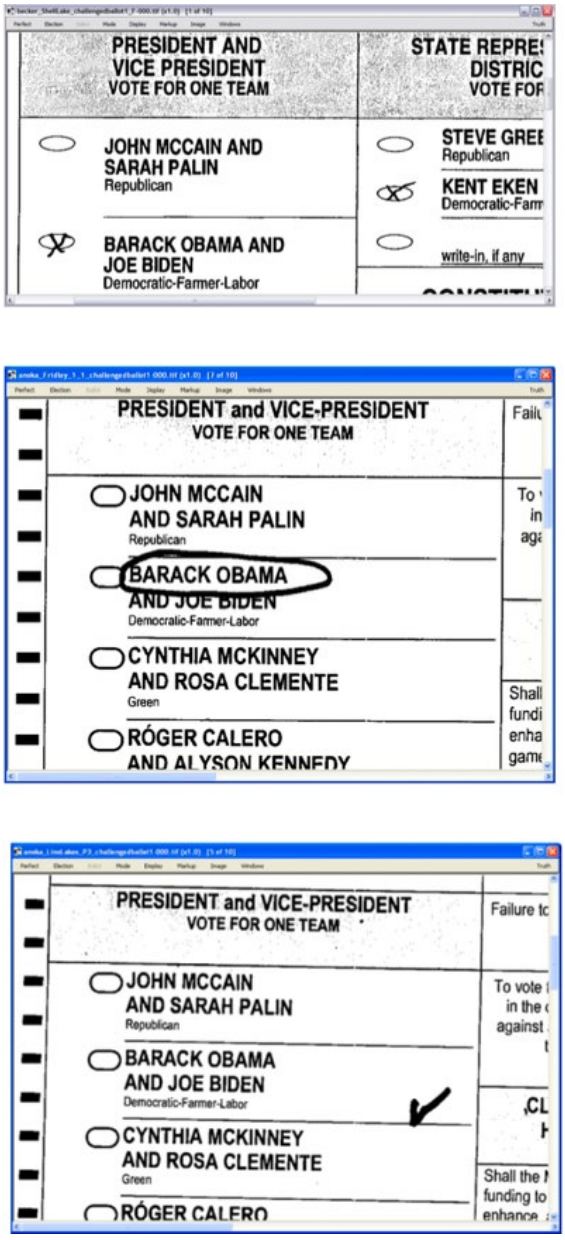

Figure 1: Non-Conforming Marking Styles[60]

Depicts 3 marked ballots submitted by voters in Minnesota wherein the voter used a marking style unrecognized by optical scan ballot readers. In this case, a circle or checkmark was used rather than the correct filling in of the candidate's bubble.

[60] Lopresti, Daniel, George Nagy, and Elisa Barney Smith. "Document Analysis Issues in Reading Optical Scan Ballots." In *Proceedings of the 9th IAPR International Workshop on Document Analysis Systems*, 105–12. Boston, MA: Association for Computing Machinery, 2010.

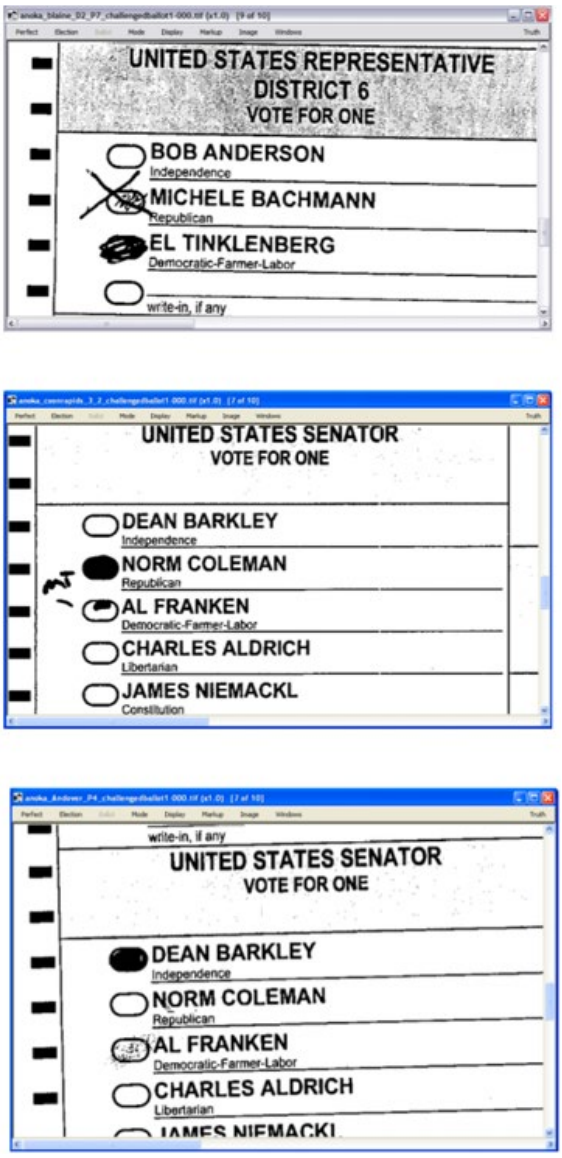

Figure 2: Attempts to Cancel a Vote[61]

Depicts three marked ballots submitted by voters in Minnesota wherein the voter attempted to cancel their vote for one candidate, resulting in the cancellation of the ballot entirely.

[61] Ibid.

Bibliography

"A Sampling of Recent Election Fraud Cases from Across the United States." The Heritage Foundation. Washington D.C. Accessed March 26, 2021. https://www.heritage.org/voterfraud/search.

Appel, Andrew W., Richard A. DeMillo, and Philip B. Stark. "Ballot-marking devices cannot ensure the will of the voters." *Election Law Journal: Rules, Politics, and Policy* 19, no. 3 (2020): 432-450.

Bernhard, Matthew, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and Alex Haldermann. "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?," University of Michigan, n.d.

Caputo, Deanna D, Shari Lawrence Pfleeger, Jesse D Freeman, and M Eric Johnson. "Going Spear Phishing: Exploring Embedded Training and Awareness." *IEEE Security & Privacy* 12, no. 1 (August 26, 2013): 28–38. https://doi.org/10.1109/MSP.2013.106.

Danetz, Lisa. "Mail Ballot Security Features: A Primer." The Brennan Center for Justice, October 16, 2020. https://www.brennancenter.org/our-work/research-reports/mail-ballot-security-features-primer.

Desilver, Drew. "Most Mail and Provisional Ballots Got Counted in Past U.S. Elections – but Many Did Not." Pew Research Center. Pew Research Center, November 10, 2020. https://www.pewresearch.org/fact-tank/2020/11/10/most-mail-and-provisional-ballots-got-counted-in-past-u-s-elections-but-many-did-not/.

Desilver, Drew. "On Election Day, Most Voters Use Electronic or Optical Scan Ballots." Pew Research Center, November 8, 2016. https://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/.

"Electronic Poll Books | e-Poll Books." National Conference of State Legislatures, October 25, 2019. https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx.

Fessler, Pam, and Johnny Kauffman. "Trips To Vegas And Chocolate-Covered Pretzels: Election Vendors Come Under Scrutiny." National Public Radio, May 2, 2019. https://www.npr.org/2019/05/02/718270183/trips-to-vegas-and-chocolate-covered-pretzels-election-vendors-come-under-scruti.

Hines, Debbie. "New Republican Data Shows No Need For Voter ID Laws." Huffington Post, February 11, 2012. https://www.huffpost.com/entry/voter-fraud-statistics_b_1139085.

"HTTP Responses." IBM. International Business Machines, February 7, 2021. https://www.ibm.com/docs/en/cics-ts/5.3?topic=protocol-http-responses.

Korte, Andrea. “AAAS' EPI Center Shares the Science of Election Security,” Science Magazine. AAAS, June 28, 2019.

Lamond, James, and Jeremy Venook. “Blunting Foreign Interference Efforts by Learning the Lessons of the Past.” Center for American Progress, September 2, 2020. https://www.americanprogress.org/issues/security/reports/2020/09/02/489865/blunting-foreign-interference-efforts-learning-lessons-past/.

Lee, Michelle Ye Hee. “What's the Difference Between Absentee and Mail-In Voting?” Washington Post. Washington Post, August 18, 2020. https://www.washingtonpost.com/politics/2020/08/18/whats-difference-between-absentee-mail-in-voting/.

Levitt, Justin. Rep. *The Truth About Voter Fraud*. New York City, NY: Brennan Center for Justice, 2007.

Lopresti, Daniel, George Nagy, and Elisa Barney Smith. “Document Analysis Issues in Reading Optical Scan Ballots.” In *Proceedings of the 9th IAPR International Workshop on Document Analysis Systems*, 105–12. Boston, MA: Association for Computing Machinery, 2010.

Martin, Michael C., and Monica S. Lam. "Automatic Generation of XSS and SQL Injection Attacks with Goal-Directed Model Checking." In *USENIX Security symposium*, pp. 31-44. 2008.

McDaniel, P., Matt Blaze and G. Vigna. “EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing.” (2007).

National Academies of Sciences, Engineering, and Medicine 2018. Securing the Vote: Protecting American Democracy. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.

Newkirk, Vann R. “How Voter ID Laws Discriminate.” The Atlantic, February 18, 2017. https://www.theatlantic.com/politics/archive/2017/02/how-voter-id-laws-discriminate-study/517218/.

Newman, Lily Hay. “Voting App Flaws Could Have Let Hackers Manipulate Results.” Wired. Condé Nast, February 13, 2020. https://www.wired.com/story/voatz-voting-app-security-flaws/.

Norden, Lawrence, and Andrea Córdova McCadney. “Voting Machines at Risk: Where We Stand Today.” Brennan Center. Brennan Center for Justice, March 5, 2019. https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-where-we-stand-today.

“Provisional Ballots.” National Conference of State Legislatures, September 17, 2020. https://www.ncsl.org/research/elections-and-campaigns/provisional-ballots.aspx.

“Risk-Limiting Audits.” National Conference of State Legislatures, February 2, 2020. https://www.ncsl.org/research/elections-and-campaigns/risk-limiting-audits.aspx.

Rivest, Ronald L. “On the notion of 'software independence' in voting systems.” Philosophical transactions. Series A, Mathematical, physical, and engineering sciences vol. 366,1881 (2008): 3759-67. doi:10.1098/rsta.2008.0149

Shalini, S., and S. Usha. "Prevention Of cross-site scripting attacks (XSS) on web applications in the client side." International Journal of Computer Science Issues (IJCSI) 8, no. 4 (2011): 650.

“States That Permit Voters to Correct Signature Discrepancies.” National Conference of State Legislatures, September 21, 2020. https://www.ncsl.org/research/elections-and-campaigns/vopp-table-15-states-that-permit-voters-to-correct-signature-discrepancies.aspx.

The Editorial Board, “The 2020 Election Won’t Look like Any We’ve Seen Before,” *The New York Times*, March 21, 2020, https://www.nytimes.com/2020/03/21/opinion/sunday/coronavirus-vote-mail.html.

US House of Representatives Committee on House Administration, and Matt Blaze. Document, 2020 Election Security - Perspectives from Voting System Vendors and Experts § (2020).

United States Senate Select Committee on Intelligence. Report, 1 Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views §. 116-290 (116AD).

“Voter Identification Requirements.” National Conference of State Legislatures. National Conference of State Legislatures, August 25, 2020. https://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx.

“Voting Outside the Polling Place: Absentee, All-Mail and Other Voting at Home Options.” National Conference of State Legislatures, September 25, 2020. https://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx.

Weiser, Wendy R, and Harold Ekeh. “The False Narrative of Vote-by-Mail Fraud.” The Brennan Center. Brennan Center for Justice, April 10, 2020. https://www.brennancenter.org/our-work/analysis-opinion/false-narrative-vote-mail-fraud.