ELECTION INTEGRITY: A PRO-VOTER AGENDA

By Myrna Pérez

BRENNAN CENTER
FOR JUSTICE
TWENTY YEARS

at New York University School of Law

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin American ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from ending mass incarceration to preserving Constitutional protection in the fight against terrorism. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, the courts, and in the court of public opinion.

ABOUT NEW IDEAS FOR A NEW DEMOCRACY

This is a moment for fresh thinking — and rethinking — new approaches to reform. The Brennan Center is committed to serving as a source for the next generation of policy innovation. New Ideas for a New Democracy is a Brennan Center series featuring unique ideas to transform our systems of democracy, justice, and the rule of law.

ACKNOWLEDGEMENTS

The Brennan Center gratefully acknowledges the Change Happens Foundation, Changing Horizons Fund of the Rockefeller Family Fund, John F. Cogan Jr., Democracy Alliance Partners, The Ralph and Fanny Ellison Charitable Trust, Ford Foundation, the Irving Harris Foundation, The Charles Evans Hughes Memorial Foundation, the Joyce Foundation, The JPB Foundation, the Karsten Family Foundation, the John D. and Catherine T. MacArthur Foundation, the Mertz Gilmore Foundation, Nancy Meyer and Marc Weiss, Open Society Foundations, the Bernard and Anne Spitzer Charitable Trust, Barbra Streisand, and the Vital Projects Fund for their generous support of our voting work.

Brennan Center President Michael Waldman deserves the main credit for this analysis. This report was his inspiration, and his vision, thinking, and writing is reflected on every page. Research and Program Associates Nelson Castaño and Erin Kelley deserve special acknowledgment for their research, drafting, fact-checking, and editing assistance. Kwame Akosah and Jonathan Brater took on a major fact-checking and editing role. Adam Gitlin and Sophie Schuit provided fact-checking and editing assistance vital to the project's completion. Larry Norden, Chris Famighetti, and Michael Li provided instrumental editorial feedback, along with Shreya Sunderaam and Suprita Dulta. Courtney McKinney and Mikayla Terrell hunted down hard-to-find sources. Legal interns Michael McDonald and Kathryn Hess edited and fact-checked. Democracy Program Director Wendy Weiser provided leadership, vision, and strategic insight throughout the drafting process.

The author thanks Jim Lyons, Erik Opsal, Jeanine Plant-Chirlin, and Desire Vincent for their invaluable editorial and production assistance, and John Kowal for his contributions to the Brennan Center's voting work.

Finally, the author would like to extend heartfelt appreciation to the experts who provided technical insight and expertise. Their work and experience, which was so willingly and graciously shared, forms the backbone of this analysis.

ABOUT THE AUTHOR

Myrna Pérez is Deputy Director of the Democracy Program at the Brennan Center for Justice, where she leads the Voting Rights and Elections project. She has authored several nationally recognized reports and articles related to voting rights, including *Election Day Long Lines: Resource Allocation* (September 2014), and *If Section 5 Fails: New Voting Implications* (June 2013). Her work has been featured in media outlets across the country, including *The New York Times, The Wall Street Journal,* MSNBC, *The Christian Science Monitor,* and the Huffington Post. Prior to joining the Center, Ms. Pérez was the Civil Rights Fellow at Relman & Dane, a civil rights law firm in Washington, D.C. Ms. Pérez graduated from Columbia Law School in 2003, where she was a Lowenstein Public Interest Fellow. Following law school, Ms. Pérez clerked for the Honorable Anita B. Brody of the United States District Court for the Eastern District of Pennsylvania and for the Honorable Julio M. Fuentes of the United States Court of Appeals for the Third Circuit. Ms. Pérez earned her undergraduate degree in Political Science from Yale University in 1996. She obtained a master's degree in public policy from Harvard University's Kennedy School of Government in 1998, where she was the recipient of the Robert F. Kennedy Award for Excellence in Public Service. Prior to law school, she was a Presidential Management Fellow, serving as a policy analyst for the United States Government Accounting Office where she covered a range of issues including housing and health care.

ELECTION INTEGRITY: A PRO-VOTER AGENDA

I. Introduction

In the weeks before the 2016 election there were charges of election rigging, attacks on state voter registration databases, and concerns of manipulation of our election results by Russian hackers. Even months after the election, and despite his attorneys' claims to the contrary,[1] President Donald Trump has claimed that millions of people voted illegally. On January 25, 2017, he stated that he would request a "major investigation" into voter fraud.[2] Trump's remarks follow on the heels of many pitched battles in the states in recent years over the right to vote. Since the 2010 election, about half of the states have passed new laws making it harder for voters to access the ballot box,[3] with proponents asserting these laws were justified because of the need to combat voter fraud.[4]

To no surprise, many of these allegations, and policies supposedly justified by them, have met vigorous and vocal opposition.[5] Opponents, including the Brennan Center, argue that many of these laws are unnecessary and harmful, placing burdensome obstacles in the path of law-abiding citizens who want to exercise their franchise.

The clamor should not obscure a fundamental shared truth: Our elections should be secure and free of misconduct. Throughout American history, political actors have tried to bend the rules and tilt the outcomes. The dangers come not so much from *voter fraud* committed by stray individuals, but from other forms of *election fraud* engineered by candidates, parties, or their supporters. Fraud, when it exists, has in many cases been orchestrated by political insiders, not individual voters. Even worse, insider fraud has all too frequently been designed to lock out the votes and voices of communities of voters, including poor and minority voters.

Election integrity need not be a euphemism for voter exclusion. Those who care about securing the right to vote and enhancing democracy in America care deeply about ensuring the honesty of elections, and avoiding misconduct. All who are eligible to vote should be able to do so in free and fair elections — but only those eligible to do so. It is vital that we protect voters from the *real* threats to the integrity of elections. Fortunately, it is possible to protect election integrity without disenfranchising eligible voters. This report proposes solutions that vary in approach. All target fraud risks as they actually exist. None will unduly disenfranchise those who have the right to vote.

A History of Misconduct by Political Actors

American history has been marked by misconduct and abuse from political insiders. From the beginning, the Framers warned that America's electoral machinery was vulnerable to political "factions." During the Constitutional Convention, James Madison warned:

"It was impossible to foresee all the abuses that might be made of the discretionary power [by state officials]. Whether the electors should vote by ballot or [by voice], should assemble at this place or that place; should be divided into districts or all meet at one place, [should] all vote for all the representatives; or all in a district vote for a number allotted to the district; these & many other points would depend on the Legislatures, and might materially affect the appointments. Whenever the State Legislatures had a favorite measure to carry, they would take care so to [mold] their regulations as to favor the candidates they wished to succeed."[6]

Madison's concerns over corruption accompanied the raw contests for power that marked much of the development of American democracy.

For example, Boss Tweed's infamous Tammany Hall Democratic machine in 19th century New York City was famed for physically dragging challengers and poll watchers out of the polls,[7] asking groups of voters to vote in multiple locations,[8] and controlling the counters who reported election results.[9] The Martin Scorsese film "Gangs of New York" accurately portrays one practice: Tammany Hall operatives would send men to vote multiple times, donning different looks each time — once fully bearded, once after shaving the sides, once with a mustache, and once more as a clean-shaven voter.[10]

Beyond colorful examples of fraud and ballot box stuffing, American history is replete with even more consequential examples of election misconduct that directly blocked citizens from voting. In the post-Reconstruction South, white Southern terrorist groups like the "White Liners," and other armed ex-Confederates, would patrol polling places, intimidate, and even murder black voters.[11] Black voters who pledged to support Democrats received "certificates of loyalty," protecting them and their families from violence and loss of employment.[12] Stuffing the ballot box to ensure Democratic victories became a "national scandal."[13] Once control of Southern state legislatures were obtained, Democrats would call for constitutional conventions to cement legal suffrage restrictions such as poll taxes, literacy tests, and property requirements.[14] At the 1890 Mississippi convention, a leading Democratic delegate conceded, "it is no secret that there has not been a full vote and a fair count in Mississippi since 1875."[15]

The 20th century saw its own share of vivid insider improprieties. For example, in 1948, Lyndon Johnson overcame a 20,000-vote deficit to win the Democratic primary by 87 votes after supporters "found" a box of votes — alphabetized and containing the same handwriting, with the same ink — all cast for him.[16] Additionally, several jurisdictions reported "corrections" to their returns.[17] Court records revealed election counters provided Johnson with extra votes by rounding out the "7" in "765" into a "9" to give Johnson 965 votes instead.[18] Rumors of misconduct long lingered. It is widely believed that John F. Kennedy's 1960 presidential victory was due to theft, notwithstanding numerous investigations finding no widespread fraud that would have changed the result.[19]

In fact, American elections grew cleaner over time. The professionalization of election administration, the decline of political machines, stronger penalties, the universal use of the secret ballot, and other factors have succeeded in greatly minimizing the incidence of many of the most notorious practices.[20]

Yet pockets of misconduct remain. The examples cited most heatedly by proponents of new voting restrictions often refer to absentee ballot fraud or other schemes orchestrated by insiders. The most dramatic recent example of such fraud came in the 1997 Miami mayoral election. Incumbent Joe Carollo won 51 percent of the votes at polling places, but 61 percent of absentee ballots were marked for the challenger, Xavier Suarez. That was enough to deny Carollo a majority vote and force a runoff nine days later that Suarez won. Carollo sued, claiming fraud. Citing "a pattern of fraudulent, intentional and criminal conduct" regarding absentee ballots,[21] the first judge to hear the case threw out the results and called for a new election.[22] An appellate court voided all the absentee ballots and declared Carollo the winner.[23] In all, 36 people, including a member of the city's code enforcement board and

a chamber of commerce president, would be charged with absentee ballot fraud to benefit several candidates in the race. The head of the local prosecutor's public corruption unit called it "a well-orchestrated conspiracy to steal the election."[24]

It is important to note what is not happening: widespread in-person voter impersonation. Admittedly, this year, numerous press outlets noted that two voters — a woman in Iowa and a man in Texas — attempted to vote for Donald Trump twice, but neither report indicated that these people were trying to impersonate another voter.[25] In fact, a comprehensive search of federal and state records and news accounts by News21, an investigative reporting program headquartered at the Walter Cronkite School of Journalism at Arizona State University, found only 10 cases of voter impersonation fraud nationwide from 2000 to 2012.[26] Overall, the group found 2,068 individual cases of alleged voter fraud,[27] but these also included "a dozen different kinds of election illegalities and irregularities."[28] An analysis of U.S. Department of Justice records showed that between 2002 and 2005 no more than two dozen people were convicted of, or pleaded guilty to, illegal voting.[29] Many of them may have voted by mistake (as when individuals who are temporarily barred from voting due to a felony conviction wrongly believe their rights have been restored).[30] As one Wisconsin federal judge noted, given the high penalties for casting even a single improper vote, a citizen would have to be "insane" to commit that crime.[31] Statistically, an individual is more likely to be killed by lightning than to commit in-person voter fraud.[32]

Toward Election Integrity

This history strongly suggests two overarching principles that should guide any further efforts to secure election integrity. Such efforts should have two key elements:

- First, they should target abuses that actually threaten election security.
- Second, they should curb fraud or impropriety without unduly discouraging or disenfranchising eligible voters.

Efforts that do not include these elements will just result in burdens to voters with little payoff.

The Brennan Center has conducted extensive research and published numerous analyses, legal briefs, case studies, and reports on the topic of fraud and security risks in election administration for over a decade. This report not only benefits from those experiences, but includes an extensive literature search to incorporate the latest research on election integrity. Additional information and confirmation of the reforms proposed here came from more than a dozen experts across an array of fields consulted for this report.

We are unwavering in our belief that the integrity of elections can be improved while protecting democracy for all. It is a false choice to say that secure elections must come at the price of voter exclusion. The solutions proposed in this report vary in their approach. Some use technology, some use enforcement, and some use common sense. But they all target fraud risks *as they actually exist.* Elections will never be truly free, fair, and accessible if precious resources are spent protecting against phantom threats. In part, the purpose of this report is to move beyond all the shopworn arguments about election integrity. Instead, it offers an election integrity reform agenda that truly protects democracy without disenfranchising legitimate voters.

II. A Pro-Voter Election Integrity Agenda

One: Modernize Voter Registration to Improve Voter Rolls

Voter registration rolls are full of inaccuracies. According to a 2012 report by the Pew Center on the States, approximately 24 million records contain errors — one in eight registrations.[33] And approximately 1.8 million dead people remained on the rolls.[34] About 2.75 million people had registrations in more than one state.[35] In 2016 the Pew Center reported improved procedures in many states since its 2012 report,[36] but problems remain. Inaccurate rolls cause confusion, expense, and disenfranchisement. They also create security risks because they are more vulnerable than clean rolls to bad actors trying to exploit out-of-date entries (for example, by voting under a person's name or mailing a ballot for someone who is lawfully voting somewhere else). Inaccurate voter rolls also fuel the perception that the system is vulnerable to fraud and undermine public confidence in our elections. Indeed, Trump surrogate Jason Miller cited the Pew report as one of two studies supporting Trump's claim that he would have won the popular vote "if you deduct the millions of people who voted illegally."[37] Errors on the rolls are not proof that ineligible individuals are voting, but they are unsurprising given the current registration system.

Today, the U.S. voter registration system relies heavily on non-governmental actors to garner names for the voter lists: individuals themselves, political parties, or nonprofit groups. A certain number of errors are to be expected under such a system. ACORN, for example, attracted criticism and controversy in 2008 when some of its paid voter registration canvassers gathered false names, and even though the group flagged suspicious registrations, they were legally required to submit them to election officials.[38] What's needed is a paradigm shift: The government should assume the duty of registering voters and maintaining complete and accurate voter registration lists. A big problem to tackle is the reliance on outdated technology, specifically ink and paper, to register voters. Paper systems may introduce typos or other mistakes as officials decipher often-illegible handwriting from thousands of forms and then type in registration information. Additionally, paper forms may be lost or damaged when transferred from office to office or by mail.

For example, in 2005, a state political party issued a report to the state attorney general's office claiming there were thousands of individuals who voted more than once, voted in multiple states, or voted while deceased.[39] A subsequent analysis of that report found that it was much more likely that election officials made mistakes entering data from paper forms, there were multiple people with the same name and birthdate, and there were duplicative registrations.[40] This episode demonstrates the risk to public confidence that comes from an error-prone and antiquated registration system.

A paradigm shift and modern technology can solve many of the problems of our registration system:

Automatic Registration. Automatic registration puts the responsibility on the government to ensure that eligible voters are registered accurately, using reliable information from government lists. This approach has two main features. First, it presumes that all eligible citizens should be registered, while allowing those who do not wish to be registered to stay

off the rolls. This feature shifts the default presumption, and that shift has a significant impact. Today, an eligible unregistered voter must take affirmative steps to get on the rolls: find a voter registration form, fill it out, and submit it to an appropriate government agency. But under automatic registration, the government registers voters and keeps those registrations up to date when voters conduct their business at government agencies unless a citizen chooses not to register. To emphasize, automatic registration is not compulsory registration. A citizen can always decline. The second feature of automatic registration is that voter information is transferred digitally from a government agency to election authorities. This method, called electronic registration, has numerous advantages over transmitting registration information by paper. It reduces errors on voter rolls attributable to illegible handwriting and typos. Electronic registration also makes it easier to build a more complete and accurate voter registration list from information in other government lists, such as Selective Service or tax records. Furthermore, the evidence shows that electronic registration not only boosts registration rates, it saves money.[41] As of February 1, 2017, at least 34 states use, or will soon use, electronic registration at Departments of Motor Vehicles (DMVs).[42]

Breakthroughs in Automatic Registration. In an important step, six states in the past two years have approved automatic voter registration — Oregon, California, Vermont, West Virginia, Connecticut, and most recently Alaska.[43] These states will automatically register voters who interact with certain government offices, changing what was once an "opt-in" system to an "opt-out" system and requiring these offices to electronically transfer information collected from voters to election officials. In Oregon, the first state to pass the reform, the new system added more than 225,000 people to voter rolls before the 2016 general election, and nearly half of them voted.[44] And in California, the nation's most populous state, automatic registration could put a large dent in the more than 6 million people who are eligible but unregistered to vote, according to California Secretary of State Alex Padilla.[45] The New Jersey and Illinois legislatures also passed automatic registration,[46] but governors in both states vetoed the reform.[47]

Portability. Registration should move with voters within a state as long as they remain eligible. Many are unaware of what's necessary to stay registered after a move. For example, one in four voters wrongly believes their registration automatically updates when they change their address with the Postal Service.[48] Portable registration allows voters who move to update their addresses with a state agency such as the DMV or a social service agency, and then sync those updates with the voter rolls. Even with these processes in place, some address updates will be missed. An Election Day mechanism would ensure full statewide portability: (1) same-day registration, in which voters can submit address changes at the polling place when they go to vote on Election Day, or (2) provisional ballots for voters who have moved, which include a space on the provisional ballot envelope for voters to provide an updated address, and which are counted unless the voter is found ineligible. Changes then should be reflected on the voter list for future elections. States with portable registration (for example, Maryland) have seen slight increases in turnout.[49] Portable registration increases election integrity by preventing eligible voters from dropping off the voter rolls and making registration lists accurate and up to date because the government will process voters' address updates right up until the ballot is cast.

Online Registration. States should create a secure and accessible online registration portal. The online system would prompt all information needed to complete a registration — the same information voters currently provide on paper. Registered voters could also use the portal to view and update their records and find polling locations, making it a full-service, one-stop shop for everything a citizen needs to cast a ballot that counts. Online registration has some integrity-enhancing features that paper-based registration systems lack. First, online registration avoids the errors associated with deciphering handwriting when entering data from paper forms. Second, online registration can also minimize duplicate registrations by flagging a matching record already in the database, and then prompting the voter to enter any address change, correction, or missing information, such as party affiliation. Tammy Patrick, a former election official and a past commissioner of the Presidential Commission on Election Administration (PCEA), notes a further advantage: officials can track where online registrations are coming from (e.g., particular IP addresses), and how quickly they arrive, which permits monitoring for fraudulent activities.[50] With paper-based registration, election officials and third-party registration groups can get thousands of forms dropped off at once, making tracking of sources more burdensome. As of January 31, 2017, at least 39 states plus the District of Columbia allow or will soon allow certain voters to register online.[51]

Election Day Fail-Safe. Eligible voters should have secure, fail-safe procedures to correct mistaken information at the polls. Even with the best and most modern list-building practices, some errors are inevitable and some voter registrations will fall through the cracks. No eligible American should lose the right to vote because of errors or omissions. Sixteen states and the District of Columbia offer or will soon offer same-day registration at the polls or an election official's office.[52] Permitting voters to correct information on Election Day is one more method for ensuring that registration rolls are accurate. In fact, one political scientist has estimated that 25 percent of the people who benefit from Election Day registration are voters who have moved.[53] Election Day registration also appears to boost turnout. In the 2016 election, the six states with the highest turn-out offered citizens the opportunity to register and vote on the same day.[54]

Two: Ensure Security and Reliability of Our Voting Machines

The hanging chads in the 2000 election Florida recount prompted a national debate about voting technology. Using $2 billion supplied by the 2002 Help America Vote Act,[55] states replaced outdated mechanical machines with computer-based voting systems. New devices proliferated. Some were precinct count optical scans, in which ballots are marked by hand and then fed into a machine.[56] Others were direct-recording electronic systems (DREs) with paper trails: Voters mark their choice on the machine and also receive a paper record of their selections.[57] Some were DREs without paper records.[58] In addition, central counters are used to tally mail-in ballots.[59] These new machines were projected to be more accurate than their predecessors.[60] But before long the reliability of the new voting systems was being called into question. A 2008 *New York Times* report on touch-screen machines noted that "in hundreds of instances" they "fail unpredictably, and in extremely strange ways; voters report that their choices 'flip' from one candidate to another before their eyes; machines crash or begin to count backwards; votes simply vanish."[61]

More recently, in the early voting period before Election Day 2016, voters in Georgia, Nevada, North Carolina, Tennessee, and Texas reported vote flipping problems.[62] On Election Day, Detroit notably had discrepancies between machine ballot counts and numbers of voters in the poll books in nearly 400 precincts, according to reports,[63] and one county in Utah had nearly 75 percent of its machines fail.[64]

These malfunctions are troubling and undermine public confidence in elections. In today's highly partisan political climate, where accusations of "rigging" abound,[65] dysfunctional voting machines breed mistrust and cynicism.

Of even greater direct concern: Although altering the outcome of a U.S. presidential election would require breaching numerous different voting systems in a country with thousands of election jurisdictions,[66] today's generation of voting machines remains vulnerable to deliberate manipulation. In 2016, the Department of Homeland Security and the Federal Bureau of Investigation released a joint analysis report linking malicious cyber activity to Russia, an unprecedented finding for such a report.[67]

A decade ago, the Brennan Center convened a task force of the nation's leading experts on voting technology and computer security. They concluded that all of the new systems "have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, state, and local elections."[68] In an era when corporate and government databases are hacked routinely — with as many as 150 million people affected in a single theft[69] — it may be only a matter of time before voting systems are penetrated. And the small number of people required to perform such a task would make Boss Tweed envious. "One attacker," the Brennan Center task force found, "need not know much about the particulars of the election or about local ballots to create an effective attack program."[70] Stanford University computer science professor David Dill argues that today's voting machine technology is susceptible to two significant risks. First, as technology becomes more complex and sophisticated it becomes harder to know when it is operating securely. More secure technology is harder to use, more difficult to understand, and might prevent officials from verifying that it has not been compromised. Second, no computer software can guarantee protection against insider attacks by those who produce or run the technology.[71]

Compounding the security and reliability problems is the age of voting machines. Electronic voting machines have shorter lifespans than mechanical ones, and machines purchased a decade ago are simply wearing out. For instance, no one expects a laptop to last 10 years. In 2014, the bipartisan PCEA, chaired by former Romney campaign counsel Benjamin Ginsberg and former Obama White House Counsel Robert Bauer, called aging voting technology an "impending crisis."[72] Because of the Help America Vote Act, many states purchased new machines at roughly the same time. Now, many are reaching the end of their useful lives. In 2015 the Brennan Center consulted more than 100 election officials and several dozen technology experts and published an alarming study, *America's Voting Machines at Risk,* finding that the majority of states are relying on aging and outdated voting machines.[73] Specifically:

- 42 states are using some machines that are at least 10 years old. In most of these states, the majority of election districts are using machines that are at least 10 years old.
- In 13 states, machines are 15 or more years old.
- Nearly every state is using some machines that are no longer manufactured.[74]

Election officials must try to maintain these machines. Some resort to cribbing parts from eBay. And even when parts can be found, the fact that they come from another era is obvious. "When we purchased new Zip Disks in 2012, they had a coupon in the package that expired in 1999," an Ohio election official told the Brennan Center.[75]

To compound the problem, the U.S. Election Assistance Commission (EAC), the independent, bipartisan federal agency responsible for developing voting-system standards,[76] has not updated certification standards since 2005. Without updated standards, jurisdictions wishing to purchase new machines are limited to EAC-certified models built with decade-old technology.[77] In response to this problem, the bipartisan PCEA called on the EAC to update its certification process and allow jurisdictions to adopt modern and more accessible voting machines.[78]

Unfortunately, as state and local governments grapple with strapped budgets, replacing these machines has not been a legislative priority. Thus far Congress has not provided federal dollars for the task.[79]

Nonetheless, there are measures that should be taken that can make voting systems more secure and reliable:

Validate and Verify Machine Accuracy and Security Before Election Day. Voting machines, including hardware and software, should be tested under conditions that mirror those on Election Day. These tests can detect problems such as software bugs and perhaps catch malicious programming. They are especially important in jurisdictions that do not provide the kinds of records that make meaningful audits possible after Election Day. Election Day inspections should also be conducted. Machines themselves should be designed so that an audit would accurately detect a malfunction.[80]

Require Post-Election Audits. Many machines now issue a paper record of a voter's selection.[82] But these records are of little security value without audits to ensure that vote tallies recorded by a particular machine match any paper records.[83] Despite near universal expert agreement on the need for audits,[84] some vendors have vigorously

Voter-Verified Records

Voting systems should provide a record that can be checked by the voter for accuracy before the ballot is submitted. Today, these records take two forms: The voter creates a record she can verify when she fills out her ballot by hand before the ballot is fed into an optical scanner. Alternatively, an electronic machine provides a paper record the voter can verify against her intended vote. By themselves, these voter records do little to enhance security. But these records are a powerful tool for audits and help show voters their choices were recorded accurately.[81]

opposed these paper trails, contending that they increase costs and slow the voting process.[85] Security experts also recommend that states pass laws for effective "risk-limiting audits." These require examination of a large enough sample of ballots to provide statistically "strong evidence that the reported election outcome was correct — if it was."[86] Also, the audit process should not rely on any one individual who might be in a position to manipulate either the voting machine or the recount device.[87] According to experts, these insider attacks are the most difficult to stop.[88] Voting technology experts also say machines must be "software independent," which is technically defined as when "an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome."[89] But practically speaking, this means that the election results can be captured independently of the machine's own software.[90] Auditors should be assigned randomly to further ensure the process is not being gamed.[91] Finally, audits should be as transparent as possible. This not only is essential to garnering public confidence, but can show a defeated candidate that she lost the election in a contest that was free and fair.[92]

Recounts and Audits.

Recounts and audits are related in that both seek to ensure the election process is working as it should. Recounts, like those Green Party candidate Jill Stein pursued in Michigan, Wisconsin, and Pennsylvania in 2016,[93] repeat the process of tabulating the votes cast to determine whether the initial count was accurate, and generally only occur when the outcome of an election contest is close.[94] Audits seek to validate and verify the accuracy of the election process. But unlike recounts, audits do not require a candidate or voter to initiate the process.[95] Audits are also much less expensive than recounts, as they involve regularly reviewing a smaller sample of ballots from a randomly selected precinct.[96] While some states require regular post-election audits, many states, including Michigan, do not.[97] In some states, including Pennsylvania, older voting machines do not have paper trails, complicating audit efforts.[98] Even in states that do require regular post-election audits, like Wisconsin,[99] these processes could be much more robust.[100]

Have Plans to Cope With Election Day Machine Failures. Any audit, test, or inspection would be of limited value if there is no agreed upon way to respond quickly if a problem is identified. Each jurisdiction should have a contingency plan in place to cope with machine problems on Election Day.

Create a National Clearinghouse of Voting Machine Issues. The EAC is responsible for certifying voting machines.[101] It has recently taken several steps to publicize information about voting system malfunctions, like an unresponsive touch screen[102] or errors with a machine's security system, for example,[103] particularly for EAC-certified voting systems.[104] However, the EAC did not certify its first voting machine until 2009, well after many jurisdictions had purchased new machines.[105] Many of the machines reaching the end of their lives are not EAC-certified.[106] A repository of data on machine problems, including those of non-EAC-certified voting systems, could be critical in preventing the same problem from occurring in multiple jurisdictions.[107] The EAC should modify its procedures so that voting system malfunctions are disclosed as soon as they are reported, making clear that the report is under investigation.

A current and comprehensive database of machine problems would provide election officials with the information they need to correct problems before an election. By keeping a log of problems, such a clearinghouse would aid officials looking to purchase new systems.

Provide Funding to Replace Unreliable Voting Machines. There appears to be little political will at the state or federal level to replace voting machines nearing the end of their life.[108] In fact, election officials in 22 states have told the Brennan Center they want to purchase new machines by 2020, but lack the funds to pay for them.[109] The Brennan Center estimates the cost of replacing the nation's aging voting equipment may exceed $1 billion.[110] With such investments looming, new machine purchases should be planned properly and include important considerations such as maintenance. If money is not allocated to replace the aging voting infrastructure, the risk that Election Day failures can affect election outcomes only grows.

Three: Do Not Implement Internet Voting Systems Until Security is Proven

In recent years lawmakers in more than 30 states have introduced legislation to use some form of Internet voting.[111] Voting by Internet is seductive because of its convenience, and fits neatly alongside all the other activities now done online such as shopping, banking, travel reservations, or even finding a partner. And it seems intuitively obvious that Internet voting would boost turnout.

Yet, some of the biggest skeptics of Internet voting are computer security experts. Jeremy Epstein, senior computer scientist at SRI International (a nonprofit technical research institute), has testified at a congressional forum that the "vast majority of computer scientists, including nearly all computer security experts, are of the opinion that internet voting cannot be done securely at this time, and probably not for another decade or more."[112] Existing technology, as well as some of the limitations in the very architecture of the Internet, makes online voting a dubious prospect. Whatever the problems of today's voting machines, they are not networked or connected to each other.[113] By contrast, the central element of the Internet is precisely its networking capability. While this characteristic makes the Internet immensely powerful, it also makes it astonishingly vulnerable from an election integrity standpoint.

Proponents argue that Internet voting would be useful for military personnel overseas,[114] would help disabled voters,[115] and is potentially cheaper[116] than traditional methods. They also point to studies indicating it might increase participation.[117] Some note that Estonia, with a population about the size of New Hampshire's,[118] uses Internet voting.[119] And some even propose a system of "televoting" that would use webcams to allow voters and election officials to monitor each other.[120] Most conspicuously, proponents note that the Internet is already used for numerous governmental and private transactions requiring security, from banking to health care[121] to air traffic control.[122]

But the security required for voting online is higher than for buying a book from Amazon. The privacy of each voter must be protected and each vote must be counted accurately. The recent high-profile cyberattacks on Sony Pictures, Target, insurer Anthem Health, internet company Dyn, the U.S. Office of Personnel Management, voter registration databases in Illinois and Arizona, and others underscore the fact that private sector and major federal agency computer networks, which have many more resources than local election administrators, are far from invulnerable.[123]

Internet fraud is already a large problem. Online retailers alone lost an estimated $3.5 billion in revenue from fraud in 2012, which was up 30 percent from 2010.[124] Less spectacularly, banks regularly replenish funds lost to online fraud in order to maintain public confidence.[125]

If jurisdictions were to switch to Internet voting, election integrity concerns in the United States could take on an international dimension. In 2010, the District of Columbia ran a pilot project in which the public was invited to attack a proposed Internet voting system. The system was quickly hacked by a team led by University of Michigan professor J. Alex Halderman. The group found it could change ballots and violate voters' secret ballot rights. They also had control of the system's network, allowing them to watch how the system was configured and tested. The penetration was so complete they even tapped into security cameras to watch system operators. Perhaps most troubling, the Michigan team found evidence of attempted break-ins that appeared to be from China and Iran. It was unclear if these attempts specifically targeted the D.C. system, but it was a chilling demonstration of the vulnerabilities of Internet voting.[126]

David Jefferson, a computer scientist at Lawrence Livermore National Laboratory, a federal research facility, warns against some of the predictable — and not necessarily easy to prevent — lines of attack on Internet voting systems:

- Readily available and customizable malware can penetrate voters' home computers, tablets, and cellphones, and steal or manipulate votes.[127]

- Denial of service attacks can shut down the entire system or target specific areas, preventing large groups of voters from voting for an extended time. Even if the system was fortified to protect against the manipulation of individual ballots, an attacker could simply delete them.[128] These attacks allow hackers to access all documents available on a computer's server.[129] Jefferson adds that these sorts of attacks are hard to prevent and can go undetected.[130]

Moreover, current resources are often inadequate to guard against increasingly sophisticated threats. Attacks can take place from anywhere in the world,[131] making detection and punishment more difficult.[132] These computer system attack techniques are constantly evolving, and current technology has limited capability in guarding against unknown threats. More than 430 million new unique pieces of malware were discovered in 2015 alone, up 36 percent from the year before, according to a study by Symantec, a cybersecurity company.[133] The Conficker worm is but one example of a virus that has successfully infiltrated millions of computers.[134] Conficker was particularly pernicious because infected computers were readily available to carry out instructions that a hacker could send remotely.[135] New exploitable weaknesses are discovered regularly on the Internet.[136]

Finally, system vulnerabilities imperil voter privacy and ballot integrity. Hackers can make "receipts" pop up on the voter's screen that appear to reflect a voter's true preference while still transmitting a different vote.[137] Accuracy notwithstanding, any receipt that recorded a citizen's vote could be used to verify that somebody voted the way they promised, enabling schemes to buy, track, or influence votes.[138]

Technologists generally agree that the following conditions should be met before implementing any Internet voting system:[139]

All Internet Voting Systems Should Allow Voters to Check that Their Vote Was Properly Cast, Recorded, and Tallied.[140] According to computer science experts convened by the U.S. Vote Foundation in 2015, "[n]o existing commercial Internet voting system is open to public review. Independent parties cannot verify that these systems function and count correctly, nor can they audit and verify election results."[141] Security experts stress that Internet systems should be "end-to-end verifiable" (E2E-V), which means that voters and auditors can see that voter choices were recorded and counted properly. It is called "end-to-end" because the goal is to protect the integrity throughout the entire process from the beginning point — the voter's intended selection — to the endpoint — the final tally.[142] One advantage of E2E-V is that it allows the public at large to independently verify vote counts while concealing the identities of individual voters through complex encryption technology.[143] While E2E-V shows promise, it is not ready to be deployed. Further research is needed to improve certain aspects of E2E-V, including anonymity protection and usability. Guaranteeing voter anonymity — while enabling voters to track their own votes — poses a unique challenge that has not yet been fully overcome.[144] Of course, any E2E-V system should also be auditable, offering verification methods clear enough that they can serve as court-admissible evidence if needed for disputed elections.[145] While a self-interested vendor may claim to offer a secure and verifiable E2E-V system, only an expert in cryptographic voting can support or debunk the vendor's assertion.[146]

Internet Voting Systems Should Not Be Unveiled for the First Time in a High-Turnout Election. There should be widespread testing, and those tests need to be in real-world environments, but real-world risks need to be managed. This can be facilitated by studying vulnerabilities from previous Internet voting tests and convening election officials, independent security experts, and technologists for advice on the feasibility of creating secure systems, risks, and needed countermeasures before rolling out such systems.[147] The experts should be comfortable that any particular proposed Internet voting system is free of glaring security vulnerabilities. The tests should be designed with as much transparency as practicable so that others beyond officials and testing labs have the opportunity to demonstrate weaknesses. This calls for publicizing the system's code, and for numerous public and live tests.

Internet Voting Systems Must Be Tested Rigorously and Continuously Because Threats Are Constant and Evolving. No amount of testing can prove a system is secure against any and all attacks. Election officials should be clear as to the limits of conclusions that can be drawn from any one evaluation or test. Even if a well-designed test shows that a system lacks certain vulnerabilities, "the lack of evidence of problems is not strong evidence that a system is safe,"[148] notes professor J. Alex Halderman, whose team, as discussed, successfully hacked the D.C. Internet voting system. Nevertheless, experts have recommendations on what testing should probe and how it should occur. What to explore in testing is relatively straightforward: the usability of the system, the ability to detect and recover from attacks, and the nature of the evidence the system can provide to verify the accuracy of a vote.[149] The test should include clear guidelines about what constitutes "success" before a trial starts.[150]

Internet Voting Systems Should Be Usable and Accessible. The usability of Internet voting systems remains a major problem. E2E-V systems, while the most promising among Internet voting options, can add complexity to the voting process, reducing usability. By way of illustration, a 2014 study of E2E-V systems found "that a significant number of voters failed to cast a ballot with each of these three systems, rendering them ineffective. Many of those voters thought they had successfully cast a ballot, only to discover that the process had failed them."[151] Usability is a prerequisite for voters, but systems must also be comprehensible for election officials. Usability issues arise in part because of the difficulty of effectively explaining to voters and election officials the complex encryption technology that makes the systems work.[152] A useable system allows problems to be better identified and unsubstantiated fears about inaccurate votes to be better assuaged.[153]

Four: Adopt Only Common-Sense Voter Identification Proposals

Many words have been used — on the floors of state legislatures, in news accounts, and legal briefs — on the issue of strict new voter identification policies. "Strict" means having a very narrow list of accepted identity documents that millions of eligible Americans do not have. In 2010, only two states had these laws.[154] Between 2011 and 2014, nine states passed strict photo ID laws, and four more limited the number of IDs a voter could show before being given a regular ballot.[155] As of mid-January 2017, 16 states were considering strict voter ID legislation — with likely more to come.[156]

Perhaps strict voter ID laws would not be so controversial if they were merely ineffective yet benign. But they are not. In fact, strict voter ID laws place barriers in front of the ballot box for many eligible Americans.[159] A Brennan Center survey showed that up to 11 percent of eligible voters — more than 21 million citizens — do not have the kind of identification required by these strict laws.[160] Additionally, many of these strict ID laws impose burdens that fall hardest on minorities, the poor, and the elderly.[161]

Strict photo ID requirements are typically not imposed in voting systems with greater security vulnerabilities, such as mail-in balloting.[157] This has raised questions about the motives of those advocating for strict photo ID rules at the polls.[158]

Given the stakes, it is no surprise that strict photo ID laws have been challenged in court. In the months preceding the 2016 general election, there were high-profile cases in three states. Federal judges blocked Texas and North Carolina from enforcing their strict photo ID requirements as enacted.[162] As a result, North Carolina did not require voters to present ID at the polls in November, while Texas offered an alternative option for those without the required ID.[163] Wisconsin's requirement remained largely intact with some court-ordered remedies for students with expired IDs and people that could not get free voter IDs. [164] The Texas law — the strictest in the nation when passed — has now been struck down by four courts, including a district court that found that more than 608,000 actual registered voters lacked the required identification.[165]

Yet some form of photo identification seems sensible to many Americans given how hard it is to maneuver through modern life without one.[166] There are ways to meet integrity concerns without disenfranchising eligible citizens. These include:

Allow Alternatives to Strict Photo Identification. There are multiple alternatives to strict photo identification laws. Some states, such as Michigan, will accept an affidavit from any voter who cannot present one of the accepted identifications, allowing the voter to cast a regular ballot.[167] Louisiana also accepts an affidavit and matches information on the affidavit against the voter rolls to verify the voter's identity.[168] Other states, like Rhode Island, request photo identification, but if a voter cannot provide one, the voter is given a provisional ballot that is tallied if the voter's identity is confirmed through a signature match.[169] As a result of the 2016 court decision discussed above, a Texan who did not have an accepted ID, and faced a barrier to obtaining one, could vote a regular ballot by presenting a secondary form of ID and signing an affidavit.[170] (There were numerous complaints that Texas did not implement the court requirements properly, however.)[171]

Some states have explored the idea of taking photos at the polls for voters without photo ID. New Hampshire has already started taking photos of voters without identification. Voters complete an affidavit and then have their picture taken and printed.[172] Democratic Secretaries of State Ross Miller of Nevada and Mark Ritchie of Minnesota have proposed taking pictures at the polls of those without photo ID and then storing the images for use in future elections.[173] But such electronic storage and retrieval of voters' images would likely also require the use of electronic poll books. Electronic poll books have many advantages, but they are an expense in a time of budgetary constraints, costing anywhere from $800 to $2,000 each in recent examples in two states.[174]

Still others suggest verifying voter identity in even more high-tech ways, such as through fingerprints[175] or other biometrics, although this verification generally happens at registration. At least 25 sub-Saharan nations have held elections using biometric voter registrations,[176] as have countries in Asia[177] and Latin America.[178] The application in this country could be, for example, taking a photo and fingerprint of the voter during the registration period. The voter could then be issued an ID card that could also be used on Election Day to verify the voter's identity. This kind of model may require biometric voter registration kits to issue the voter ID cards,[179] which would be a radical change from the way registration has been done in the United States.[180] For one thing, the government would need to take over responsibility for voter registration from the nonprofit groups, parties, and candidates who currently register a large percentage of voters.[181] Registration also would need to be done at centralized locations where the equipment needed to capture biometrics could be kept.[182] In the Philippines, where biometrics are used to register voters, voter registration generally requires a trip to a government office.[183] And in states that are implementing automatic registration, like California,[184] moving to a biometric requirement would mean adding a step before voters' registrations became effective.[185] Moreover, like any machine, these kits can break down. In Kenya, in 2012, some of these breakdowns lasted as long as two weeks.[186] Biometric machines are also necessary to read fingerprints at the time of voting. In the 2012 presidential election in Ghana, failures and delays caused by these machines were so widespread that the government added an extra day for voting in what was supposed to be a one-day election.[187] These systems also incur expenses. For instance, the cost of issuing biometric identity cards in Côte d'Ivoire for the 2010 election was more than $44 per voter.[188]

Ensure Every Eligible Voter Has the Identification Required to Vote. Strict identification requirements are disenfranchising because not every eligible American has an accepted ID. If everyone did, the disenfranchising effects of these laws would narrow considerably.[189] So if a state requires documentary identification to vote, the state must also take steps necessary to ensure that every eligible citizen has the required identification. Experience shows that supplying the necessary identification to voters requires having a sufficient number of trained and skilled government employees to assist those who need help, whether navigating the bureaucratic path, obtaining or collecting records, or getting to a government agency.[190] Another baseline requirement is waiving costs for any accepted identification document and the documents (such as birth certificates) needed to obtain them.[191] Yet, these efforts will be meaningless unless poll workers are adequately trained about the identification requirements, how to enforce the ID laws evenly and accurately, and how to meaningfully assist voters who appear at the polling location without the required ID.[192] This is particularly important where state-issued election manuals grant poll workers discretion in deciding whether someone is who he or she claims to be.[193]

Five: Increase Security of Mail-In Ballots

A growing number of states have adopted vote-by-mail regimes. In 1984, only five states allowed vote-by-mail elections.[194] As of 2016, at least 22 states conducted some or all of their elections by mail.[195] Although voters still have the option of going to a polling place or election office, Washington, Oregon, and Colorado conduct all of their elections primarily by mail,[196] while 19 other states allow voters to submit their ballots by mail in certain elections.[197] In fact, all states, and D.C., permit mail voting in connection with absentee voting.[198] While a complete accounting of this year's ballots will take time, the Election Assistance Commission found that mail-in ballots accounted for more than 25 percent of all votes cast in the 2014 election, and more than 20 percent of those cast in 2012.[199]

The appeal of vote-by-mail is no mystery. In addition to the convenience for voters,[200] some research suggests vote-by-mail systems save money because jurisdictions no longer have to hire as many poll workers.[201] There are also some studies indicating mail balloting regimes increase turnout (although there are other studies with contrary findings).[202]

Yet vote-by-mail raises election integrity issues because of concerns that ballots can be filled out improperly or manipulated for ballot stuffing. "[V]otes cast by mail are less likely to be counted, more likely to be compromised and more likely to be contested than those cast in a voting booth," statistics show. Election officials reject almost 2 percent of ballots cast by mail, double the rate for in-person voting, wrote *The New York Times* in 2012.[203] In 2014, 2.1 percent of domestic absentee ballots were returned undeliverable, 0.6 percent were spoiled, and 1.4 percent were rejected.[204]

In fact, the first known cyberattack on a voting system involved mail-in ballots.[205] In 2012, a Miami grand jury revealed that a "clandestine, untraceable computer program" had submitted more than 2,500 online requests for mail-in absentee ballots by voters who had not requested them.[206] The scheme was uncovered after the county's vendor became suspicious when it appeared that an extraordinary number of absentee ballot requests were coming from the same computer and being submitted at a rate that was not humanly possible.[207] The mastermind

behind the crime was never found.[208] And in Fort Worth, Texas, a woman pleaded guilty in 2012 to using absentee ballots to vote under five different names.[209] A search of News21's database of all election fraud cases from 2000-2012 shows that about 25 percent of them involved mail-in balloting.[210]

On a related, but different note, MIT professor Charles Stewart III notes that there are numerous opportunities for a mail-in ballot to be lost. At the beginning, a request for a mail-in ballot might not be received. Even after officials process the request, the voter might not receive the requested ballot. Finally, election officials might not receive the completed mail-in ballot, assuming it is filled out properly.[211] "The opportunities to lose votes appear to be greater along the mail route than along the in-person route," Stewart notes.[212]

Given their convenience and purported lower costs, vote-by-mail systems are only likely to grow in popularity. Election officials should focus on the following two areas to bolster security and to minimize lost votes:

Improve Security at Each Stage of the Mail-In Ballot Pipeline. Each stage of the mail-in ballot pipeline has vulnerabilities, from ensuring security at the printer to verifying that requests for absentee ballots are only made by eligible and registered voters to collecting the ballots in a secure location.[213] Fortunately, technology can alleviate some of these concerns. Just as Federal Express and Amazon use bar codes to track a package at each step in the process, at least some jurisdictions in Washington, Colorado, and Oregon use ballot tracking systems with bar codes (sometimes referred to as "Intelligent Mail Barcodes" or "IMB") that allow both voters and election officials to see where a ballot is, be it in a mail truck, drop box,[214] or election office.[215] Knowing where the ballot is at any point is critical to the chain of custody and in achieving integrity in the process, says Tammy Patrick, the former election official, who also served on the U.S. Postal Service's Mailer's Technical Advisory Committee.[216]

Use Best Practices for Signature Verification. Washington, Colorado, and Oregon use signature matches to protect integrity.[217] In Oregon, the secretary of state's office outlines the characteristics to be looked for by election officials reviewing signatures and the signature reviewers receive the same training as law enforcement professionals.[218] In Washington, election workers receive signature-matching training[219] from a state patrol fraud unit.[220] In Colorado, signatures are examined by election judges from both political parties.[221]

Six: Protect Against Insider Wrongdoing

All states have laws to guard against election fraud — for example, voting more than once in an election, buying votes, and intimidating voters.[222] Election fraud with respect to both registration and voting is also a federal crime that can result in fines of up to $5,000 and up to five years in prison.[223] These serious penalties should deter many casual wrongdoers. But politicians and party officials often have their very livelihoods — or quest for power — at stake in elections, boosting their incentives for misconduct. It is not surprising that many instances of election fraud, both historically and in the present day, involve the actions of insiders. Recent abuses by insiders have included lawmakers lying about where they live,[224] magistrate judges willfully registering ineligible persons,[225] and legislators running fraudulent absentee ballot schemes.[226] In 2013, a pollworker in Ohio was famously found guilty of using her authority and training to conduct voter fraud and take certain steps to evade

detection.[227] Culprits have even included the chief election officer of Indiana.[228] This is why election officials and workers should receive special attention because their insider status increases their opportunity to both abuse the system and avoid detection.[229] Moreover, when organizational leaders are involved in wrongdoing, it can create a culture for fraud, encouraging others to commit misconduct.[230]

Some common practices from the private sector to prevent fraud can be used by election administrators and law enforcement. Among them:

Have Effective Preventative Controls. As an initial matter, election workers should be fully aware of their responsibilities, the laws governing them, and the penalties for failing to do so.[231] Experts agree that when the leadership of an organization shows that it is committed to integrity and punishing fraud, the chance that another insider will commit fraud decreases.[232] More concrete prevention measures include: segregating duties among employees so that one person does not have too much authority over sensitive transactions, implementing a tiered system of authorization or clearance such that only certain people can do certain tasks, and using appropriate physical controls such as locks, keys, safes, fences, and guards.[233]

Make Detection Swift and Certain. Swift detection is important because when a fraudulent act is unnoticed, the perpetrator becomes emboldened and is likely to commit more fraud.[234] Good record keeping, sensible transparency procedures, and frequent audits or reviews are all basic tools election administrators can employ to detect fraud.[235] However, the internal controls must be well-designed and followed because "[p]eople know when they are not being watched, and when the auditor is not diligent in what they are doing."[236] Also, there should be sufficient resources for independent or outside review of senior officials because "perpetrators with higher levels of authority are typically in a better position to override controls or conceal their misconduct."[237]

Tip lines enabling anonymous reporting of misconduct are used often in the private sector, and they are now beginning to be deployed in election administration. Today, some states including Georgia, Florida, and Louisiana have hotlines to report suspected voter fraud.[238] The president of the Association of Certified Fraud Examiners, James D. Ratley, CFE, recommends that the tip line be open to election administrators and the public, and operated by a neutral party and staffed by well-trained operators who know how to collect the necessary information while protecting caller anonymity.[239] But information gathering means little unless leads are investigated properly. Investigators should have the necessary resources to probe alleged misconduct and sufficient training to detect election fraud, including instruction on how to ensure an investigation is not compromised or distracted by political partisans.

Make the Punishment Public. Publicity about those who commit fraud is an important element of any prevention effort. Instead of perhaps hiding known fraud in an effort to avoid embarrassment, knowledge of fraud activity should be made widely known. The reason is that fraud detection, in and of itself, acts as a deterrent. Joseph Wells, an accountant and former FBI agent who specializes in fraud, notes that "[w]hile [internal] controls are necessary, that isn't what really deters fraud; it's the *perception of detection*. Succinctly stated, those who perceive that they will be caught committing fraud are less likely to commit it."[240] A belief that fraud will be uncovered may be especially important in the election context. Because many of those who perpetrate fraud are high-level managers or those in public leadership positions, public punishment is more salient as it might not only result in criminal liability but also irreparable harm to reputation.[241]

Conclusion

We do not have to choose between election integrity and election access. Indeed, free and fair access is necessary for an election to have integrity. This report examined genuine risks to the security of elections, highlighting current vulnerabilities as well as those that will be faced in the future. Recommendations have been made about how to reduce each risk. We invite and urge policymakers to tackle these problems.

ENDNOTES

1 Donald J. Trump and Donald J. Trump for President, Inc.'s Objections to Dr. Jill Stein's Recount Petition at 2, In re *Petition for Recount for the Office of President of the United States of America* (State of Michigan Board of State Canvassers, filed Dec. 1, 2016) ("All available evidence suggests that the 2016 general election was *not* tainted by fraud or mistake"); Application to Dismiss by the Republican Party of Pennsylvania, All Pennsylvania Electors of President-Elect Donald J. Trump and Vice-President-Elect Michael Pence, President-Elect Trump, Vice-President-Elect Pence, and Donald J. Trump for President, Inc., In re: *2016 Presidential Election*, No. 659 MD 2016, at 2-3 (Commonwealth Ct. of Pa., filed Dec. 1, 2016) ("There is no evidence-or even an allegation-that any tampering with Pennsylvania's voting systems actually occurred....The absence of any evidence of tampering is no surprise.").

2 Jonathan Weisman & Steve Eder, *Trump Promises 'Major Investigation' of Voter Fraud in 2016 Election*, N.Y. Times, Jan. 25, 2017, *available at* https://www.nytimes.com/2017/01/25/us/politics/donald-trump-administration.html.

3 For example, some state legislatures cut same-day registration, reduced early voting, enacted strict photo ID laws, and demanded that voters present documentary proof of citizenship when registering to vote. *See* Wendy Weiser & Erik Opsal, Brennan Ctr. for Justice, The State of Voting in 2014 1, 3 (2014), http://www.brennancenter.org/sites/default/files/analysis/State_of_Voting_2014.pdf. For a detailed survey of restrictive state laws passed since the 2010 election, see *States with New Voting Restrictions since 2010 Election*, Brennan Ctr. for Justice (July 7, 2015), http://www.brennancenter.org/sites/default/files/analysis/Restrictive_Appendix_Post-2010.pdf.

4 For example, in Texas the legislature passed the country's strictest photo identification law in 2011, and maintained in court that that the law was justified as a means to "deter and detect voter fraud, and to preserve voter confidence in the integrity of elections." Brief for Appellants (Redacted) at 38, Veasey v. Perry, No. 14-41127 (5th Cir. Jan. 29, 2015). In Alabama, voters were required to comply with a strict photo ID requirement for the first time in 2014, after years of being allowed to show non-photo ID such as social security cards and utility bills. Mike Cason, *Alabama's photo voter ID law declared a success; not everyone agrees*, AL.com (Nov. 24, 2014), http://www.al.com/news/index.ssf/2014/11/alabamas_new_photo_voter_id_la.html (last visited Dec. 9, 2015). The legislature defended its decision to tighten the voter ID law as a measure to help prevent voter fraud. *See id*. Mississippi passed a law via a citizen initiative in 2012 requiring voters to provide government issued photo ID.

5 *See, e.g.*, Stephen Ansolabehere, Samantha Luks & Brian Schaffner, *Trump wants to investigate purported mass voter fraud. We pre-debunked his evidence*, Wash. Post (Jan. 25, 2017), https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/19/trump-thinks-non-citizens-are-deciding-elections-we-debunked-the-research-hes-citing/; Justin Levitt, *A comprehensive investigation of voter impersonation finds 31 credible incidents out of one billion ballots cast*, Wash. Post (Aug. 6, 2014), http://www.washingtonpost.com/news/wonkblog/wp/2014/08/06/a-comprehensive-investigation-of-voter-impersonation-finds-31-credible-incidents-out-of-one-billion-ballots-cast/.

6 The Records of the Federal Convention of 1787, at 240-41 (Max Farrand ed., 1937).

7 *Tweed's Pretended Election*, N.Y. Times, Jan. 10, 1872, at 4, *available at* http://query.nytimes.com/mem/archive-free/pdf?res=9402E5DE1739EF34BC4852DFB7668389669FDE.

8 *See id*.

9 *See* John Fund, *How to Steal an Election*, City J. (Autumn 2004), http://www.city-journal.org/html/14_4_urbanities-election.html.

10 Andrew Gumbel, Steal This Vote: Dirty Elections and the Rotten History of Democracy in America 74-75 (2005); Gangs of New York (Miramax Film Corp. 2002).

11 *See* Nicholas Lemann, Redemption: The Last Battle of the Civil War 114-17, 124-27 (2006). The purpose of "White Line" organizations was to reestablish white Democratic control of government by violently disrupting black and Republican organizing and voting. *Id* at 80.

12 *Id.* at 170-75. Early efforts on the part of white southern Democrats to use violence and intimidation to suppress the black vote in the 1870s were taken in a manner to try and evade notice by the federal government and risk intervention by federal troops looking to enforce black voting rights. *See id*.

13 Morgan Kousser, The Shaping of Southern Politics 46-47 (1974). One tactic, employed by South Carolina and Florida Democrats, involved stuffing ballot boxes with tissue ballots and extra-small tickets nicknamed "little jokers." The unique feel and size of the fraudulent ballots ensured they were not discarded when election officials, sympathetic to the Democrats, were blindfolded and asked to randomly remove by hand the number of ballots in excess of the number of voters in the jurisdiction. *Id.*; *see also* Kate Kelly, Election Day: An American Holiday, an American History 129 (2008).

14 *See* Kousser, *supra* note 13, at 39-40 (explaining how Democrats used voter fraud to realize legal voter suppression). For a detailed history of Southern suffrage restrictions introduced at the various post-Reconstruction disenfranchising conventions, see *id*. at 45-62.

15 *Id*. at 47.

16 Pamela Colloff, *Go Ask Alice*, Tex. Monthly, Nov. 1998, at 22, *available at* http://www.texasmonthly.com/politics/go-ask-alice/; Martin Tolchin, *How Johnson Won Election He'd Lost,* N.Y. Times, Feb. 11, 1990, at A30, *available at* http://www.nytimes.com/1990/02/11/us/how-johnson-won-election-he-d-lost.html.

17 Tolchin, *supra* note 16, at A30.

18 *See* Robert A. Caro, The Years of Lyndon Johnson: Means of Ascent 360 (1990).

19 David Greenberg, *Was Nixon Robbed?*, Slate (Oct. 16, 2000), www.slate.com/articles/news_and_politics/history_lesson/2000/10/was_nixon_robbed.html.

20 *See generally* Michael Waldman, The Fight to Vote 97-114 (2015) (discussing Progressive Era election reforms).

21 Mireya Navarro, *Fraud Ruling Invalidates Miami Mayoral Election*, N.Y. Times, Mar. 5, 1998, at A1, *available at* http://www.nytimes.com/1998/03/05/us/fraud-ruling-invalidates-miami-mayoral-election.html.

22 Scheer v. City of Miami, 15 F. Supp. 2d 1338, 1340 (S.D. Fla. 1998); Navarro, *supra* note 21.

23 *In re* Protest Election Returns and Absentee Ballots in November 4, 1997 Election for City of Miami, Fla., 707 So. 2d 1170, 1175 (Fla. 3d Dist. Ct. App., 1998); *Florida Appeals Court Returns Defeated*

Mayor of Miami to Post, N.Y. Times, Mar. 12, 1998, at A16, *available at* http://www.nytimes.com/1998/03/12/us/florida-appeals-court-returns-defeated-mayor-of-miami-to-post.html.

24 Luisa Yanez, *21 Charged In Miami Absentee Vote Fraud*, SunSentinel, Oct. 29, 1998, at 3B, *available at* http://articles.sun-sentinel.com/1998-10-29/news/9810280191_1_absentee-ballots-voter-fraud-miami-dade-county-jail.

25 Both individuals were arrested, according to media reports. *See* Alex Samuels & Jim Malewitz, *Problems at the polls: Some Texas voters see long waits, machine glitches*, Tex. Tribune, Nov. 8, 2016, *available at* https://www.texastribune.org/2016/11/08/voting-issues-texas/; Amy B. Wang, *Trump supporter charged with voting twice in Iowa*, Wash. Post, Oct. 29, 2016, *available at* https://www.washingtonpost.com/news/post-nation/wp/2016/10/29/trump-supporter-charged-with-voting-twice-in-iowa/. As of the publication of this document, hearings were pending.

26 *Exhaustive Database of Voter Fraud Turns Up Scant Evidence That It Happens*, News21 (Aug. 12, 2012), http://votingrights.news21.com/article/election-fraud-explainer/index.html.

27 *See Election Fraud in America*, News21 (Aug. 12, 2012), http://votingrights.news21.com/interactive/election-fraud-database/.

28 *See Exhaustive Database of Voter Fraud Turns Up Scant Evidence That It Happens*, *supra* note 26.

29 Lorraine C. Minnite, Ph.D., Project Vote, The Politics of Voter Fraud 8 (2007), *available at* http://www.projectvote.org/wp-content/uploads/2007/03/Politics_of_Voter_Fraud_Final.pdf.

30 *See*, *e.g.*, Eric Lipton & Ian Urbina, *In 5-Year Effort, Scant Evidence of Voter Fraud*, N.Y. Times, Apr. 12, 2007, at A1, *available at* http://www.nytimes.com/2007/04/12/washington/12fraud.html.

31 Frank v. Walker, 17 F. Supp. 3d 837, 850 (E.D. Wis. 2014).

32 *See* Justin Levitt, Brennan Ctr. for Justice, The Truth About Voter Fraud 6 (2007), *available at* http://www.brennancenter.org/sites/default/files/legacy/The%20Truth%20About%20Voter%20Fraud.pdf.

33 Inaccurate, Costly, and Inefficient: Evidence that America's voter Registration System Needs An Upgrade, Pew Ctr. on the States 1 (2012), *available at* http://www.pewtrusts.org/~/media/legacy/uploadedfiles/pcs_assets/2012/pewupgradingvoterregistrationpdf.pdf; *see also* Levitt, *supra* note 32, at 4.

34 Pew Ctr. on the States, *supra* note 33, at 1.

35 *Id.*

36 Alexis Schuler & Samuel Derheimer, *Upgrading Voter Registration Processes*, Pew Charitable Trusts, Oct. 18, 2016, *available at* http://www.pewtrusts.org/en/research-and-analysis/analysis/2016/10/18/upgrading-voter-registration.

37 Michelle Ye Hee Lee, *Trump camp's repeated use of dubious sources on voter fraud*, Wash. Post, Nov. 29, 2016, *available at* https://www.washingtonpost.com/news/fact-checker/wp/2016/11/29/trump-camps-repeated-use-of-dubious-sources-on-voter-fraud.

38 Jess Henig, *ACORN Accusations*, FactCheck.org (Oct. 18, 2008), http://www.factcheck.org/2008/10/acorn-accusations/.

39 David Chen, *Among Voters in New Jersey, G.O.P. Sees Dead People*, N.Y. Times, Sept. 16, 2005, at B5, *available at* http://www.nytimes.com/2005/09/16/nyregion/among-voters-in-new-jersey-gop-sees-dead-people.html.

40 Brennan Ctr. for Justice & Michael McDonald, Analysis of the September 15, 2005 Voter Fraud Report Submitted to the New Jersey Attorney General (2005), *available at* http://brennan.3cdn.net/9d1efbddb2c45834e0_pom6bx3bk.pdf.

41 *See, e.g.,* Telephone Interview with Howard Snider, Dir. of Voter Servs., South Carolina State Election Commission (Apr. 10, 2013); Telephone Interview with Brandon Johnson, Senior Elections Coordinator, S.D. Sec'y of State (Apr. 5, 2013). For example, in Maricopa County, Arizona (which includes Phoenix), processing a paper voter registration form costs 83 cents, while processing applications received electronically costs an average of 3 cents. *See Voter Registration Modernization in the States*, Brennan Ctr. for Justice (Dec. 1, 2015), http://www.brennancenter.org/analysis/voter-registration-modernization-states.

42 *See Voter Registration Modernization in the States, supra* note 41.

43 *Automatic Voter Registration*, Brennan Ctr. for Justice (Nov. 9, 2016), https://www.brennancenter.org/analysis/automatic-voter-registration.

44 Searom England, *Oregon Motor Voter Registers More Than 270,000 Voters Through November*, Or. Sec'y of St. (Dec. 12, 2016), http://oregonsosblog.us/2016/12/oregon-motor-voter-registers-270000-voters-november/; *see also* Niraj Chokshi, *Automatic Voter Registration a 'Success' in Oregon*, N.Y. Times, Dec. 2, 2016, https://www.nytimes.com/2016/12/02/us/politics/oregon-voter-registration.html.

45 Ian Lovett, *California Law Will Automatically Register Drivers to Vote*, N.Y. Times, Oct. 10, 2015, at A14, *available at* http://www.nytimes.com/2015/10/11/us/california-law-will-automatically-register-drivers-to-vote.html.

46 Rob Duffey, *Broad Coalition Calls on Christie to Sign New Jersey Democracy Act Without Delay,* PolitickerNJ (Sept. 2, 2015), http://politickernj.com/2015/09/broad-coalition-calls-on-christie-to-sign-new-jersey-democracy-act-without-delay/; Jonathan Brater, *Nearly 1 in 5 Americans May Soon Live in a State with Automatic Voter Registration*, Brennan Ctr. for Justice (June 1, 2016), https://www.brennancenter.org/blog/nearly-1in5-americans-may-soon-live-state-automatic-voter-registration.

47 Press Release, Brennan Ctr. for Justice, Gov. Christie Vetoes Groundbreaking Voting Reform in New Jersey, (Nov. 9, 2015), *available at* https://www.brennancenter.org/press-release/gov-christie-vetoes-groundbreaking-voting-reform-new-jersey. Rick Pearson, *Rauner vetoes automatic voter registration bill*, Chicago Tribune (Aug. 12, 2016), *available at* http://www.chicagotribune.com/news/local/politics/ct-bruce-rauner-veto-automatic-voter-registration-met-0813-20160812-story.html.

48 Pew Ctr. on the States, *supra* note 33, at 7.

49 *See* Michael P. McDonald, *Portable Voter Registration*, 30 Pol. Behav. 491-501 (2008), *available at* http://link.springer.com/article/10.1007%2Fs11109-008-9055-z.

50 Telephone Interview with Tammy Patrick, Senior Advisor, Bipartisan Policy Ctr. Democracy Project (Mar. 30, 2015).

51 *Voter Registration Modernization in the States*, *supra* note 41.

52 *Same Day Voter Registration*, Nat'l Conf. St. Legislatures (Jan. 11, 2017), http://www.ncsl.org/research/elections-and-campaigns/same-day-registration.aspx. In North Carolina, same-day registration during early voting was reinstated by a court ruling in 2016.

53 *See* McDonald, *supra* note 49, at 496

54 Danielle Kurtzleben, *CHARTS: Is The Electoral College Dragging Down Voter Turnout In Your State?*, Nat'l Pub. Radio (Nov. 26, 2016), http://www.npr.org/2016/11/26/503170280/charts-is-the-electoral-college-dragging-down-voter-turnout-in-your-state (citing Michael McDonald, *2016 November General Election Turnout Rates*, http://www.electproject.org/2016g).

55 52 U.S.C. § 20901 et seq. (2012 & West Supp. 2015).

56 *See* Lawrence Norden & Christopher Famighetti, Brennan Ctr. for Justice, America's Voting Machines at Risk 8-9 (2015), *available at* https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

57 Brennan Ctr. Task Force on Voting Sys. Sec., The Machinery of Democracy: Protecting Elections in an Electronic World 2 (2006), *available at* http://www.brennancenter.org/sites/default/files/publications/Machinery%20of%20Democracy.pdf.

58 DREs without a paper trail only record and tabulate votes on the machine. *See id*.

59 *See, e.g.*, *Premier/Diebold (Dominion) AccuVote OS Central Count Scanner*, Verified Voting (Sept. 21, 2015 2:08 PM), https://www.verifiedvoting.org/resources/voting-equipment/premier-diebold/accuvote-os-cc/.

60 *See* Stephen Ansolabehere & Charles Stewart III, *Residual Votes Attributable to Technology*, 67 J. Pol. 365, 366 (2005), *available at* http://vote.caltech.edu/sites/default/files/residual_votes_attributable_to_tech.pdf.

61 Clive Thompson, *Can You Count on Voting Machines?*, N.Y. Times Mag., Jan. 6, 2008, at 40, *available at* http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html.

62 Lawrence Norden & Christopher Famighetti, *America's Aging Voting Machines Managed to Survive Another Election*, Brennan Ctr. for Justice (Nov. 10, 2016), https://www.brennancenter.org/blog/americas-aging-voting-machines-managed-survive-another-election.

63 Lawrence Norden, *Michigan Recount Exposes Voting Machine Failures*, Brennan Ctr. for Justice (Dec. 8, 2016), https://www.brennancenter.org/blog/michigan-recount-exposes-voting-machine-failures.

64 David DeMille, *Voting machine issues complicate balloting in Washington County*, The Spectrum (Nov. 8, 2016), http://www.thespectrum.com/story/news/2016/11/08/election-machine-problems-early-washington-county/93470912/?hootPostID=884417d80befb56efe41e9f9dd4005e5.

65 *See* Pam Fessler, *Some Machines Are Flipping Votes, But That Doesn't Mean They're Rigged*, Nat'l Pub. Radio (Oct. 26, 2016), http://www.npr.org/2016/10/26/499450796/some-machines-are-flipping-votes-but-that-doesnt-mean-theyre-rigged; John Tedesco, *Company acknowledges Bexar ballot glitch that omitted Greg Abbott's name*, mySA (Nov. 5, 2014), http://www.mysanantonio.com/news/local/article/Bexar-ballot-Abbott-malfunction-5873080.php#photo-7098404.

66 *See, e.g.*, David C. Kimball & Brady Baybeck, *Are All Jurisdictions Equal? Size Disparity in Election Administration*, 12 Election L.J. 130, 130 (2013), *available at* http://www.umsl.edu/~kimballd/DKBBELJ2013.pdf.

67 Dep't of Homeland Security & Fed. Bureau of Investigation, Joint Analysis Report: GRIZZLY

STEPPE – Russian Malicious Cyber Activity (Dec. 29, 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

68 Brennan Ctr. Task Force on Voting Sys. Sec., *supra* note 57, at 3.

69 Daniel Howley, *The Biggest Computer Hack Attacks of the Last 5 Years*, Yahoo! (July 31, 2015), https://www.yahoo.com/tech/the-biggest-computer-hack-attacks-of-the-last-5-125449860474.html.

70 Brennan Ctr. Task Force on Voting Sys. Sec., *supra* note 57, at 47.

71 *See* David L. Dill & Aviel D. Rubin, *E-Voting Security*, IEEE Security & Privacy, Jan.-Feb. 2004, at 22, 22, *available at* https://www.computer.org/csdl/mags/sp/2004/01/j1022.pdf; Telephone Interview with David Dill, Professor of Computer Sci. and Electrical Eng'g, Stanford Univ. (Mar. 16, 2015); *see also* Thomas W. Lauer, *The Risk of E-Voting*, 2.3 The Electronic J. of e-Government 177, 181 (2004), *available at* http://www.researchgate.net/profile/Thomas_Lauer/publication/228920801_The_risk_of_e-voting/links/004635182c0960710c000000.pdf.

72 The Presidential Comm'n on Election Admin., The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration 62 (2014), *available at* https://www.supportthevoter.gov/files/2014/01/Amer-Voting-Exper-final-draft-01-09-14-508.pdf.

73 Norden & Famighetti, *supra* note 56, at 1; *see also Voting System Security and Reliability Risks*, Brennan Ctr. for Justice (Aug. 30, 2016), https://www.brennancenter.org/analysis/fact-sheet-voting-system-security-and-reliability-risks.

74 Norden & Famighetti, *supra* note 56, at 4.

75 *Id*. at 14.

76 *About the EAC*, U.S. Election Assistance Comm'n, http://www.eac.gov/about_the_eac/ (last visited Dec. 9, 2015).

77 *See* The Presidential Comm'n on Election Admin, *supra* note 72, at 11-12.

78 *See* Letter from Benjamin Ginsberg & Robert Bauer, Co-Chairs, Presidential Comm'n on Election Admin., to Thomas Hicks, Comm'r, U.S. Election Assistance Comm'n (Dec. 19, 2014), *available at* http://bipartisanpolicy.org/wp-content/uploads/2014/12/PCEA-BPC-Voting-Technology.pdf; Letter from Benjamin Ginsberg & Robert Bauer, Co-Chairs, Presidential Comm'n on Election Admin., to Matthew Masterson, Comm'r, U.S. Election Assistance Comm'n (Dec. 19, 2014), *available at* http://bipartisanpolicy.org/wp-content/uploads/2014/12/PCEA-BPC-Voting-Technology.pdf; Letter from Benjamin Ginsberg & Robert Bauer, Co-Chairs, Presidential Comm'n on Election Admin., to Christy McCormick, Comm'r, U.S. Election Assistance Comm'n (Dec. 19, 2014), *available at* http://bipartisanpolicy.org/wp-content/uploads/2014/12/PCEA-BPC-Voting-Technology.pdf.

79 *See* Cory Bennett, *States ditch electronic voting machines*, The Hill (Nov. 2, 2014), http://thehill.com/policy/cybersecurity/222470-states-ditch-electronic-voting-machines.

80 The vulnerability of component parts is demonstrated by the recent reports on the potential to use USBs to infiltrate and sabotage computers. Computer experts have revealed that it is possible to program component parts such as USBs — and all manner of USB-enabled devices like computer mice, keyboards, and smartphones — to hack into computers. They assert that, because a simple "test"— such as deleting all of a USB's contents, which would not erase the malware — might not detect the malware, it is best

not to "connect your USB device to computers you don't own or don't have good reason to trust." Indeed, security consultants advise that devices such as USBs need to be cleared by technicians with advanced training in order to track, and disarm, certain malware. Andy Greenberg, *Why the Security of USB is Fundamentally Broken,* Wired (July 31, 2014), http://www.wired.com/2014/07/usb-security/; *see also* Andy Greenberg, *The Unpatchable Malware that Infects USBs is Now on the Loose,* Wired (Oct. 2, 2014), http://www.wired.com/2014/10/code-published-for-unfixable-usb-attack/.

81 *See* Philip B. Stark & David Wagner, *Evidence-Based Elections*, IEEE Security & Privacy, Sept.-Oct. 2012 at 33, 33; *see also* Risk-Limiting Audits Working Group, Risk-Limiting Post-Election Audits: Why and How 6-7 (2012), *available at* https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf.

82 Brennan Ctr. Task Force on Voting Sys. Sec., *supra* note 57, at 2, 4.

83 N. Ansari et al., *Evaluating Electronic Voting Systems Equipped with Voter-Verified Paper Records*, IEEE Security & Privacy, May-June 2008, at 30, 30, *available at* https://web.njit.edu/~ansari/papers/08Security&%20Privacy.pdf; *see also* Telephone Interview with Joseph Kiniry, Research Lead, Galois (Mar. 26, 2015).

84 Eric Lazarus, the principal investigator in the 2006 Brennan Center Task Force on Voting System Security, proposes one way of auditing voting machines, called SOBA (secrecy-preserving observable ballot-level audit). It consists of auditing random samples of ballots that cannot be traced to specific voters. *See* Josh Benaloh, et al., *SOBA: Secrecy-preserving Observable Ballot-level Audit*, *in* Proceedings of the 2011 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections "EVT/WOTE '11" (2011), *available at* http://statistics.berkeley.edu/stark/Preprints/soba11.pdf.

85 In 2004, Harris Miller, the president of the Information Technology Association of America, lobbied against voter verified paper trails (VVPAT), saying, " 'We oppose the idea of a voter-verified paper trail' . . . on grounds that it increases costs, slows the voting process, and may reduce reliability." G. David Garson, Public Information Technology and E-Governance: Managing the Virtual State 73 (2006); *see also* Megan Santosus, *The Lowdown on E-Voting*, CIO (July 30, 2004), http://www.cio.com.au/article/67933/lowdown_e-voting/.

86 Risk-Limiting Audits Working Group, *supra* note 81, at 2. The paper further explains, "Risk limiting audits systematically check the election outcomes reported by vote-counting systems. Specifically, a risk-limiting audit checks some voted ballots or voter-verifiable records in search of strong evidence that the reported election outcome was correct — if it was. Specifically, if the reported outcome (usually the set of winner(s)) is incorrect, then a risk-limiting audit has a large, pre-specified minimum chance of leading to a full hand count that reveals the correct outcome. A risk-limiting audit can stop as soon as it finds strong evidence that the reported outcome was correct. (Closer elections generally entail checking more ballots.)" *Id*.

87 *See, e.g.*, Thomas W. Lauer, *The Risk of e-Voting*, 2 Electronic J. of E-Government Sept. 2004, at 177, 181 (2015), *available at* www.ejeg.com/issue/download.html?idArticle=34; *see also* Kiniry, *supra* note 83.

88 *See* David Jefferson et al., *Analyzing Internet Voting Security*, 47 Comm. of the ACM, Oct. 2004, at 59, 61, *available at* https://people.csail.mit.edu/rivest/voting/reports/cacm/2004-10%20CACM%20p59%20Jefferson%20Rubin%20Simons%20Wagner%20-%20Analyzing%20Internet%20Voting%20Security.pdf; *see also* Dill, *supra* note 71; E-mail from Joseph Kiniry, Research Lead, Galois, to Nelson Castaño, Research and Program Assoc., Brennan Ctr. for Justice (Sept. 25, 2015, 14:27 EDT) (on file

with author).

89 Ronald L. Rivest, *On the Notion of 'Software Independence' in Voting Systems*, 366 Phil. Transactions of the Royal Soc'y A 3759, 3759-3761 (2008); *see also* Philip B. Stark & David Wagner, *supra* note 81.

90 Rivest, *supra* note 89, at 3759-3761; Kiniry, *supra* note 83; *see also* Stark & Wagner, *supra* note 81. Examples of software independent voting machines include, but are not limited to, DRE voting systems with voter-verified paper trails, voter-verified paper audit trail machines, and optical scan voting systems. *See* Rivest, *supra* note 89, at 3762-63.

91 *See* Tigran Antonyan et al., *State-Wide Elections, Optical Scan Voting Systems, and the Pursuit of Integrity*, 4 IEEE Transactions on Info. Forensics & Sec.597, 604 (2009), *available at* http://dx.doi.org/10.1109/TIFS.2009.2033232 (stating that the auditing process itself should be randomly audited to ensure that auditors are trustworthy); *see also* Kiniry, *supra* note 83.

92 *See* David Jefferson, *What Happened in Sarasota County?*, The Bridge, Summer 2007, at 17, 22, *available at* https://www.nae.edu/File.aspx?id=7408; *see also* Telephone Interview with David Jefferson, Computer Scientist, Lawrence Livermore Nat'l Lab. (Mar. 25, 2015).

93 Daniella Diaz, *Jill Stein defends her recount efforts*, CNN (Nov. 28, 2016), http://www.cnn.com/2016/11/28/politics/jill-stein-recount-2016-election/.

94 *See Automatic Recounts*, Nat'l Conf. St. Legislatures (Oct. 26, 2016), http://www.ncsl.org/research/elections-and-campaigns/automatic-recount-thresholds.aspx.

95 *Post-Election Audits*, Nat'l Conf. St. Legislatures (June 14, 2016), http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

96 *Id*; *Automatic Recounts*, *supra* note 94; Pew Ctr on the States, The Cost of Statewide Recounts (2010), *available at* http://www.pewtrusts.org/~/media/legacy/uploadedfiles/pcs_assets/2010/recountbrief1pdf.pdf.

97 M.C.L.A. § 168.31a.

98 Norden and Famighetti, *supra* note 56.

99 Wisc. Stat. Ann. § 7.08(6).

100 *See generally* Mark Lindeman & Philip B. Stark, *A Gentle Introduction to Risk-limiting Audits*, 10 IEEE Security and Privacy No. 5:42-49 (2012), *available at* https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

101 The EAC certifies, decertifies, and recertifies voting system hardware and software and accredits test laboratories. While states are not required to participate in the program, some have enacted laws that require some level of participation. *See* U.S. Election Assistance Comm'n, State Requirements and the Federal Voting System Testing and Certification Program 3 (2011), *available at* http://www.eac.gov/assets/1/Page/State%20Requirements%20and%20the%20Federal%20Voting%20System%20Testing%20and%20Certification%20Program.pdf.

102 U.S. Election Assistance Comm'n, EAC Certified System Technical Advisory—ESS2011-02 (2011), *available at* http://www.eac.gov/assets/1/Documents/Unity3210-Screen_Unresponsiveness.Technical_Advisory-07.28.2011-FINAL.pdf.

103 Election Sys. & Software, Loading ExpressVote Media:"Manifest Signature Verification Failed", Election Assistance Comm'n (2015), http://www.eac.gov/assets/1/Page/ESS-FYIEWR0026Rev2-07.10.2015.pdf.

104 *See* U.S. Election Assistance Comm'n, Quality Monitoring Program, http://www.eac.gov/testing_and_certification/quality_monitoring_program.aspx (last visited Dec. 9, 2015).

105 Norden & Famighetti, *supra* note 56, at 8.

106 *Id.* at 32. To be clear, this document does not maintain that EAC-certification will address all problems associated with voting machines. A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE), Public Comment on the Voluntary Voting Systems Guidelines, Version 1.1, The United States Election Assistance Comm'n 7-9 (Sept. 28, 2009), *available at* http://www.eac.gov/assets/1/workflow_staging/Page/126.PDF. At least one expert believes that the current certification standard is "far, far below" what technologists and activists on the topic wanted. E-mail from Joseph Kiniry, *supra* note 88.

107 Norden & Famighetti, *supra* note 56, at 32.

108 *See* Bennett, *supra* note 79.

109 Norden & Famighetti, *supra* note 56, at 5.

110 *Id.* at 40.

111 Barbara Simons & Douglas W. Jones, *Internet Voting in the U.S.*, 55 Comm. of the ACM, Oct. 2012, at 68, 70-71, *available at* http://cacm.acm.org/magazines/2012/10/155536-internet-voting-in-the-us/fulltext; *see also* Pamela Smith & Bruce McConnell, *Hack the Vote: Perils of the Online Ballot Box*, Verified Voting (May 30, 2014), https://www.verifiedvoting.org/hack-the-vote-the-perils-of-the-online-ballot-box-pamela-smith-and-bruce-mcconnellwall-street-journal/; *see also Electronic Transmission of Ballots*, Nat'l Conference of State Legislatures (Jan. 28, 2015), http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx. Internet voting was probably first used in the United States in 1996 by the Reform Party. In 2000, the Republican Party in Alaska and the Democratic Party in Arizona allowed voters to vote online, for the straw polls and the primaries, respectively. *See* Dimitris A. Gritzalis, Secure Electronic Voting 26 (2003); Larry Sabato & Howard R. Ernst, Encyclopedia of American Political Parties and Elections 187 (2007). In 2010, the Federal Voting Assistance Program ("FVAP") ran a test program in 17 states that encouraged eligible voters to cast their ballots online. *See Epic v. DOD (E-voting Security Tests)*, Electronic Privacy Info. Ctr., http://epic.org/foia/dod/e-voting/default.html (last visited Dec. 9, 2015).

112 Jeremy Epstein, Senior Computer Scientist, SRI International, Prepared statement of Jeremy Epstein to the Congressional Forum: "Lessons from Election Day 2012: Examining the Need for Election Reform." (Jan. 14, 2013), http://democrats.oversight.house.gov/sites/democrats.oversight.house.gov/files/migrated/Epstein_Forum_Statement_Final_011413.pdf; Scott Wolchok et al., *Attacking the Washington, D.C. Internet Voting System*, 7397 Lecture Notes in Computer Sci., Feb.-Mar. 2012, 114, 114-15, *available at* http://link.springer.com/chapter/10.1007%2F978-3-642-32946-3_10; *see generally* Joseph R. Kiniry et al., The Future of Voting: End-To-End Verifiable Internet Voting 109-10 (2015), *available at* https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf; E-mail from David Jefferson, Computer Scientist, Lawrence Livermore Nat'l Lab., to author (Sept. 24, 2015, 03:15 EDT) (on file with author).

113 Bennett, *supra* note 79.

114 *See* Ian Urbina, *States Move to Allow Overseas and Military Voters to Cast Ballots by Internet*, N.Y. Times, May 8, 2010, at A18, *available at* http://www.nytimes.com/2010/05/09/us/politics/09voting.html. To be clear, it is not in dispute that too many military voters overseas face serious difficulties in casting ballots that will count, and something should be done to address the problem. A diverse group of commentators agrees. *See, e.g.*, Hans A. von Spakovsky & M. Eric Eversole, *America's Military Voters: Re-enfranchising the Disenfranchised*, Heritage Found. (July 28, 2009), http://www.heritage.org/research/reports/2009/07/americas-military-voters-re-enfranchising-the-disenfranchised; Jared Serbu, *DoD personnel miss out on absentee ballots*, Fed. News Radio (Oct. 28, 2011), http://federalnewsradio.com/federal-drive/2011/10/dod-personnel-miss-out-on-absentee-ballots/; *see also* M. Eric Eversole, *Military voters soon to be disenfranchised—again*, Wash. Times (July 20, 2010), http://www.washingtontimes.com/news/2010/jul/20/military-voters-soon-to-be-disenfranchised-again/; Pam Fessler, *Voting Machines Are Aging, But Don't Expect Congress To Pay To Replace Them*, Nat'l Pub. Radio (Oct. 15, 2015),http://www.npr.org/sections/itsallpolitics/2015/10/15/448931114/voting-machines-are-aging-but-dont-expect-congress-to-pay-to-replace-them; Press Release, Charles E. Schumer, Schumer Releases Survey Suggesting Ballots of One in Four Overseas Military Voters Went Uncounted in '08 Election, May 13, 2009, http://www.schumer.senate.gov/newsroom/press-releases/schumer-releases-survey-suggesting-ballots-of-one-in-four-overseas-military-voters-went-uncounted-in-08-election.

115 *See* Steve Friess, *Court case: Voting via the Internet is a civil rights issue for disabled*, Al Jazeera America (July 30, 2014), http://america.aljazeera.com/articles/2014/7/30/court-case-votingviatheinternetisacivilrightsissuefordisabled.html.

116 *See* R. Michael Alvarez & Jonathan Nagler, *The Likely Consequences of Internet Voting for Political Representation*, 34 Loy. L.A. L. Rev. 1115, 1116 (2001), *available at* http://vote.caltech.edu/content/likely-consequences-internet-voting-political-representation (discussing the perception that Internet voting reduces costs). Advocates of Internet voting have also inferred that Internet voting is more cost-efficient because it would presumably cut the costs of maintaining a physical polling place. But case studies reveal that the costs of holding an election online can be greater than the costs of operating physical polling places. For example, elections held online in New South Wales, Australia cost the state over $3.5 million (Australian dollars) to implement and develop. Similarly, cost estimates for a proposal to allow overseas Internet voting in Washington ranged from $2.5 million to $4.44 million, prompting the legislature to abort the plan. Simons & Jones, *supra* note 111, at 71.

117 Part of the attraction to Internet voting comes from the belief that it can make voting more accessible to all voters. However, some have expressed concern that Internet voting may advantage wealthier voters with access to the Internet over those who do not have steady access to an Internet-connected computer or device. Multiple studies have found that Internet voting is actually more likely to be used by wealthier, younger, and well-educated voters than by their counterparts. *See* Pippa Norris, *E-Voting as the Magic Ballot?* 5-6 (Feb. 16, 2004) (unpublished paper), *available at* http://www.hks.harvard.edu/fs/pnorris/Acrobat/EUI%20E-Voting%20as%20the%20Magic%20Ballot.pdf; Daniel Bochsler, *Can Internet voting increase political participation? Remote electronic voting and turnout in the Estonian 2007 parliamentary elections* 4 (May 26, 2010), *available at* http://www.eui.eu/Projects/EUDO-PublicOpinion/Documents/bochslere-voteeui2010.pdf; Frederic I. Solop, *Digital Democracy Comes of Age: Internet Voting and the 2000 Arizona Democratic Primary Election*, 34 PS: Pol. Sci. and Politics 289, 291 (2001). Moreover, Solop, a professor of politics at Northern Arizona University, contends that Internet voting is particularly appealing to well-educated and younger voters. *See id.* at 292. Other studies indicate no evidence of a permanent effect on participation. *See* Nicole J. Goodman, Internet Voting in a Local Election in Canada 15 (2014); Simons & Jones, *supra* note 111, at 71; *see also* R. Michael Alvarez, Thad E. Hall & Alexander H. Trechsel, *Internet Voting in Comparative Perspective: The Case of Estonia*, 42 PS: Pol. Sci. & Pol. 497, 498 (2009).

118 Estonia's population is approximately 1.314 million. The World Bank Data—Estonia, http://data.worldbank.org/country/estonia (last visited Dec. 9, 2015). New Hampshire's population is approximately 1.326 million. U.S. Census Bureau–New Hampshire, http://quickfacts.census.gov/qfd/states/33000.html (last visited Dec. 9, 2015).

119 Brad Plumer, *Estonia gets to vote online. Why can't America?*, Wash. Post (Nov. 6, 2012), http://www.washingtonpost.com/blogs/wonkblog/wp/2012/11/06/estonians-get-to-vote-online-why-cant-america/. Opponents respond that a study of the Estonian Internet voting system concluded the system was insecure. Charles Arthur, *Estonian e-voting shouldn't be used in European elections, say security experts*, The Guardian (May 12, 2014), http://www.theguardian.com/technology/2014/may/12/estonian-e-voting-security-warning-european-elections-research; *see* Drew Springall et al., *Security Analysis of the Estonian Internet Voting System*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Comm'ns Sec. 703 (2014), *available at* http://delivery.acm.org/10.1145/2670000/2660315/p703-springall.pdf.

120 Dr. Juan Gilbert, Chair of the Computer & Information Science & Engineering Department at the University of Florida, has noted the advantages of such a system. Tigran Antonyan, Report on the NIST/EAC Future of Voting Systems Symposium 10 (2013), *available at* https://voter.engr.uconn.edu/voter/wp-content/uploads/NIST-EAC-Report.pdf. The voter casts a ballot over the Internet and, without looking at it, an election official shows the ballot to the voter via a webcam and submits it for processing once the voter verifies her vote is accurately reflected on the paper held by the election official. This webcam feature, in theory, allows a voter to see their ballot processed in the voting precinct. This proposal, however, has inspired strong concern from other technologists. Some warned us that systems using webcams are still not entirely trustworthy. For example, the voter may be coerced by bad actors not pictured in the camera feed. Professor Philip Stark refers to this voting system as a fiction because it may appear to some to be a solution to a problem, but in actuality it does not ensure that the voter is who they say they are, nor does it protect voter anonymity (the live video feeds can be recorded or eavesdropped on without the voter knowing). Telephone Interview with Philip B. Stark, Professor of Statistics, Univ. of Cal. Berkeley (Sept. 18, 2015); *see also* Telephone Interview with Joseph Kiniry, Research Lead, Galois (Mar. 11, 2015); E-mail from Josh Benaloh, Senior Cryptographer, Microsoft Research, to author (Sept. 22, 2015, 17:06 EDT) (on file with author).

121 Josh Catone, *How Close Are We to Internet Voting?*, Mashable.com (Oct. 2, 2012), http://mashable.com/2012/10/02/internet-voting/.

122 *See* Doug Gross, *Why can't Americans vote online?*, CNN (Nov. 8, 2011), http://www.cnn.com/2011/11/08/tech/web/online-voting/.

123 *See generally* David E. Sanger, *Five Possible Hacks to Worry About Before Election Day*, N.Y. Times (Nov. 3, 2016), https://www.nytimes.com/2016/11/04/us/politics/five-possible-hacks-to-worry-about-before-election-day.html ; Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. Times (Oct. 21, 2016), https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html; Evan Perez & Simon Prokupecz, *U.S. data hack may be 4 times larger than the government originally said*, CNN (June 24, 2015), http://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html; Lori Grisham, *Timeline: North Korea and the Sony Pictures hack*, USA Today (Jan. 5, 2015), http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/; Andrea Peterson, *The Sony Pictures hack, explained*, Wash. Post (Dec. 18, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/; Gregory Wallace, *Target credit card hack: What you need to know*, CNN (Dec. 23, 2013), http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/; Niam Yaraghi & Joshua Bleiberg, *The Anthem hack shows there is no such thing as privacy in the health*

care industry, The Brookings Institution (Feb. 12, 2015), http://www.brookings.edu/blogs/techtank/posts/2015/02/12-anthem-hack-health-privacy.

124 Paul Demery, *Online fraud costs e-retailers $3.5 billion in 2012*, Internet Retailer (Mar. 28, 2013), https://www.internetretailer.com/2013/03/28/online-fraud-costs-e-retailers-35-billion-2012.

125 Simons & Jones, *supra* note 111, at 68; *see, e.g.*, *Identity Fraud is Up, but Banks are Up to the Challenge*, Javelin Strategy & Research (Mar. 14, 2013), https://www.javelinstrategy.com/news/1399/92/Identity-Fraud-is-Up-but-Banks-are-Up-to-the-Challenge/d,pressRoomDetail.

126 Simons & Jones, *supra* note 111, at 69-70.

127 *See* David Jefferson, *If I Can Shop and Bank Online, Why Can't I Vote Online?*, Verified Voting, https://www.verifiedvoting.org/resources/internet-voting/vote-online/ (last visited Dec. 9, 2015); *see also* Telephone Interview with David Jefferson, Computer Scientist, Lawrence Livermore Nat'l Lab. (Mar. 4, 2015). Tests have shown that online election systems are widely susceptible to hacking. In 2004, a group of experts called the Security Peer Review was asked to evaluate the Secure Electronic Registration and Voting Experiment (SERVE), a project intended to allow Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) voters to register and vote online during the 2004 election cycle. The project was shut down after the computer scientists in the Security Peer Review recommended that the system not be implemented because of the "danger of successful, large-scale attacks." Simons & Jones, *supra* note 111, at 71-72. In another case, discrepancies were found in the ballot count of a 2008 test of an Internet voting pilot system designed for UOCAVA voters, Bring Remote Access to Voters Overseas (BRAVO). As of August 2012, BRAVO had not released a formal report on the discrepancies. *See id*.

128 Jaikumar Vijayan, *Internet voting systems too insecure, researcher warns,* Computerworld (Mar. 1, 2012), *available at* http://www.computerworld.com/article/2501967/security0/internet-voting-systems-too-insecure--researcher-warns.html; *see also* Jefferson, Mar. 4, *supra* note 127; Jefferson et al., *supra* note 92, at 63-64. David Jefferson and three other security experts contend that a large-scale denial-of-service attack could render an online voting service unavailable on Election Day, which would call into question the validity of the election and "effectively disenfranchise" large numbers of UOCAVA voters. Alternatively, denial-of-service attacks could knock out or degrade network services for areas where a particular demographic is known to vote for a particular party, possibly modifying the outcome of the election. Jefferson et al., *supra* note 92, at 63-64.

129 Joseph Migga Kizza, Ethical and Social Issues in the Information Age 191 (4th ed. 2010).

130 Jefferson, et al., *supra* note 92, at 64.

131 Attacks from abroad on private and public systems are common. Examples include: a group of Chinese hackers infiltrating the *New York Times*, *see* Nicole Perlroth, *Hackers in China Attacked The Times for Last 4 Months*, N.Y. Times, Jan. 31, 2013, at A1, *available at* http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html; hackers from multiple nations breaching the computer at the Department of Veterans Affairs, *see* Eric Chabrow, *VA Systems Hacked From Abroad*, Data Breach Today (June 5, 2013), http://www.databreachtoday.asia/va-systems-hacked-from-abroad-a-5814/op-1; suspicions of Chinese hackers breaching the U.S. Postal Service's computer networks, *see* Ellen Nakashima, *China suspected of breaching U.S. Postal Service computer networks*, Wash. Post (Nov. 10, 2014), http://www.washingtonpost.com/blogs/federal-eye/wp/2014/11/10/china-suspected-of-breaching-u-s-postal-service-computer-networks/; and the hacking of Microsoft and NATO by Russian hackers, Tom Risen, *Russian Hackers Target NATO, Ukraine*, U.S. News and World Report (Oct. 14, 2014), http://www.usnews.com/news/articles/2014/10/14/russian-hackers-target-nato-ukraine.

132 *See, e.g.*, Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, Sci. Am. (June 11, 2011), http://www.scientificamerican.com/article/tracking-cyber-hackers/. According to some experts, our inability to detect the infiltration of an online election system is perhaps its most serious risk. *See, e.g.*, Jefferson, Mar. 4, *supra* note 127 ("No one would ever know [if an election was compromised] . . . . The undetectability is critical.").

133 *See* 21 Symantec, Internet Security Threat Report 5 (2016), *available at* https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. According to some experts, our inability to detect the infiltration of an online election system is perhaps its most serious risk. *See, e.g.*, Jefferson, Mar. 4, *supra* note 127 ("No one would ever know [if an election was compromised] . . . . The undetectability is critical.").

134 The worm reportedly infected up to 15 million machines in 2009. Simons & Jones, *supra* note 111, at 74.

135 *See id*.

136 One recent example is the "FREAK flaw," a vulnerability in the Internet protocol used for accessing websites that allows hackers to instruct web browsers to weaken the encryption of their own information. *See*, *e.g.*, J. Alex Halderman & Vanessa Teague, *The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election*, 9269 Lecture Notes in Computer Sci., Apr. 2015, 35, 40-1, *available at* http://arxiv.org/abs/1504.05646; *see also* Craig Timberg, *'FREAK' flaw undermines security for Apple and Google users, researchers discover*, Wash. Post (Mar. 3, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/03/freak-flaw-undermines-security-for-apple-and-google-users-researchers-discover/; E-mail from J. Alex Halderman, Dir. of Ctr. for Computer Sec. and Soc'y, Univ. of Mich., to Nelson Castaño, Research and Program Assoc., Brennan Ctr. for Justice (Sept. 19, 2015, 15:39 EDT).

137 *See* Simons & Jones, *supra* note 111, at 75.

138 *See id*. at 76.

139 Many of the experts consulted for this report also contributed to a report making recommendations on E2E-V and Internet voting systems commissioned by the U.S. Vote Foundation. As a result, our recommendations are similar to those contained in that report. The report can be found here: https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf.

140 *See* Kiayias et al., *End-to-End Verifiable Elections in the Standard Model*, 9057 Lecture Notes in Computer Sci., Apr. 2015, 468, 468, *available at* http://link.springer.com/chapter/10.1007%2F978-3-662-46803-6_16.

141 Kiniry et al., *supra* note 112, at iii-iv (Executive Summary).

142 *Id.*

143 *See* Kiniry et al., *supra* note 112, at 18-41 (providing general characteristics of, as well as detailed examples of, E2E-V Internet voting systems).

144 *See id.* at 19-20; Telephone Interview with Philip B. Stark, Professor of Statistics, Univ. of Cal. Berkeley (Mar. 30, 2015).

145 Josh Benaloh et al., End-to-end verifiability 2 (2014), *available at* https://elections.virginia.gov/Files/Media/SB11Workgroup/EndtoEndVerifiabilityFeb2014.pdf; *see also* E-mail from David Jefferson, Computer Scientist, Lawrence Livermore Nat'l Lab., to author (Sept. 24, 2015, 13:24 EDT) (on file with author); Telephone Interview with J. Alex Halderman, Dir. of Ctr. for Computer Sec. and Soc'y, Univ. of Mich. (Mar. 2, 2015); *see also* Kiniry et al., *supra* note 112, at 110-11.

146 Experts are concerned that "well-meaning" legislators and election officials will "deploy Internet voting systems too early and too quickly, based on misleading information from prospective vendors . . . that is not balanced with *independent* advice from cybersecurity experts." Kiniry et al., *supra* note 112, at 107. Professor Halderman also warns that some vendors are starting to use "the terms 'E2E' and 'verifiable' to refer to much weaker protections." Halderman, *supra* note 136.

147 In 2011, the National Institute of Standards and Technology (NIST), by request of the EAC, conducted a review of online voting technologies and the existing threats for these systems. The NIST researchers found significant issues in protecting voters' computers from attacks, implementing wide scale voter authentication processes, and auditing online voting systems. They thus recommend that research and testing continue if we hope to achieve a secure online voting system. Nelson Hastings, Rene Peralta, Stefan Popoveniuc, & Andrew Regenscheid, Nat'l Inst. of Standards and Tech., Security Considerations for Remote Electronic UOCAVA Voting 1, 59 (2011), http://www.nist.gov/itl/vote/upload/NISTIR-7700-feb2011.pdf.

148 Halderman, *supra* note 145; Scott Wolchok et al., *supra* note 112, at 124 (explaining that the "lack of problems found in testing *does not* imply a lack of problems in the system").

149 *See* P.L. Vora et al., *Evaluation of Voting Systems*, 47 Comm. of the ACM, Nov. 2004, at 144, 144, *available at* http://euro.ecom.cmu.edu/people/faculty/mshamos/200411cacm-vspr-article.pdf; *see also* Halderman, *supra* note 145 (urging study of all three areas).

150 L. Jay Aceto, Michelle M. Shafer, Edwin B. Smith III & Cyrus J. Walker, *Internet Voting Security Auditing from System Development Through Implementation: Best Practices from Electronic Voting Deployments*, 205 Lecture Notes in Informatics, July 2012, 146, 150, *available at* http://www.e-voting.cc/wp-content/uploads/downloads/2014/10/20120620_EVOTE2012_Proceedings_V-final.pdf; *see also* Halderman, *supra* note 146; Jefferson, Mar. 4, *supra* note 127; Scott Wolchok et al., *supra* note 112, at 124 (noting that testers should be aware of the drawbacks inherent in a testing environment before conducting a test; for example, testers often have "more limited resources and weaker incentives compared to real attackers").

151 *See* Kiniry et al., *supra* note 112, at 28.

152 Also, studies on E2E-V show that voters do not understand how to do what they need to do for the system to be successful, and lack the motivation to learn. *See* Jeremy Epstein, End to End Cryptographic Internet Voting Considered Harmful (Oct. 14, 2009), http://csrc.nist.gov/groups/ST/e2evoting/documents/papers/EPSTEIN_TradeoffsPanel.pdf; *see also* Telephone Interview with Jeremy Epstein, Senior Computer Scientist, SRI International (Mar. 13, 2015); Telephone Interview with Josh Benaloh, Senior Cryptographer, Microsoft Research (Mar. 3, 2015); Jefferson, Mar. 4, *supra* note 127.

153 *See* P.L. Vora et al., *supra* note 149, at 144; *see also* Jefferson, Mar. 4, *supra* note 127.

154 Wendy R. Weiser & Lawrence Norden, Brennan Ctr. for Justice, Voting Law Changes in 2012, at 4, 12 (2011), *available at* http://www.brennancenter.org/sites/default/files/legacy/Democracy/VRE/Brennan_Voting_Law_V10.pdf.

155 Weiser & Opsal, *supra* note 3, at 3.

156 *Voting Laws Roundup 2017 Preview*, Brennan Ctr. for Justice (Jan. 18, 2017), https://www.brennancenter.org/analysis/voting-laws-roundup-2017-preview.

157 For example, Texas and Tennessee both recently imposed strict photo ID requirements, but these laws do not apply for absentee voters. *See, e.g.*, *Voter ID Laws Passed Since 2011*, Brennan Ctr. for Justice (Nov. 12, 2013), https://www.brennancenter.org/analysis/voter-id-laws-passed-2011. Section Five of this report goes into greater detail on the vulnerabilities of mail balloting systems. *See also* Beth Hundsdorfer & George Pawlaczyk, *Alorton trustee and Cahokia man charged with vote fraud*, Belleville News-Democrat (May 8, 2015), http://www.bnd.com/news/local/crime/article20547705.html; Alleged Miami-Dade Absentee Ballot Fraudster Agrees to a Plea Deal, Huffpost Miami (Oct. 8, 2013), http://www.huffingtonpost.com/2013/10/08/deisy-cabrera_n_4065379.html; *Voter Fraud News*, Republican Nat'l Law. Ass'n, https://www.rnla.org/votefraud.asp (last visited Dec. 9, 2015).

158 In striking down North Carolina's strict photo ID law, applicable only to in-person voting, the Fourth Circuit Court of Appeals noted that "the State has failed to identify even a single individual who has ever been charged with committing in-person voter fraud in North Carolina. On the other [hand] the General Assembly did have evidence of alleged cases of mail-in absentee voter fraud." NAACP v. McCrory, 831 F.3d 204, 235 (4th Cir. 2016) (citations omitted).

159 Matt A. Barreto, Stephen A. Nuño & Gabriel R. Sanchez, *The Disproportionate Impact of Voter-ID Requirements on the Electorate - New Evidence from Indiana*, 42 PS: Pol. Sci. & Pol. 111, 115 (2009); R. Michael Alvarez, Delia Bailey & Jonathan N. Katz, *The Effect of Voter Identification Laws on Turnout* 20 (Cal. Inst, of Tech., Soc. Sci. Working Paper No. 1267R, 2008), *available at* http://ssrn.com/abstract=1084598; *see generally* Richard Sobel, Charles Hamilton Houston Institute for Race & Justice, The High Cost of 'Free' Photo Voter Identification Cards (2014), *available at* http://www.charleshamiltonhouston.org/wp-content/uploads/2014/08/FullReportVoterIDJune2014.pdf; Nate Silver, *Measuring the Effect of Voter Identification Laws*, N.Y. Times (July 15, 2012), http://fivethirtyeight.blogs.nytimes.com/2012/07/15/measuring-the-effects-of-voter-identification-laws/.

160 Brennan Ctr. for Justice, Citizens without Proof: A Survey of Americans' Possession of Documentary Proof of Citizenship and Photo Identification 3 (2006), *available at* http://www.brennancenter.org/sites/default/files/legacy/d/download_file_39242.pdf; *see also* Wendy Weiser, Keesha Gaskins, & Sundeep Iyer, Brennan Ctr. for Justice, *Citizens Without Proof Stands Strong: A Response to Von Spakovsky and Ingram*, http://brennan.3cdn.net/1493a22ae1998b3043_78m6bndfg.pdf (last visited Dec. 9, 2015). Additionally, multiple studies have corroborated the findings of the Brennan Center's report. The percentage of voters who do not have proper identification required under strict voter ID laws varies based on demographic. For a compilation of studies on voter ID, see the Brennan Center's Research on Voter ID portal at http://www.brennancenter.org/analysis/research-and-publications-voter-id.

161 *See generally* Lonna Rae Atkeson et al., *A New Barrier to Participation: Heterogeneous Application of Voter Identification Policies*, 29 Electoral Studies 66 (2010); Veasey v. Abbott, 796 F. 3d 487, 507 (5th Cir. 2015) *available at* https://www.brennancenter.org/sites/default/files/legal-work/Fifth_Circuit_Opinion.pdf; Barreto et al., *supra* note 159; *see* Richard Sobel & Robert Ellis Smith, *Voter-ID Laws Discourage Participation, Particularly among Minorities, and Trigger a Constitutional Remedy in Lost Representation*, 42 PS: Pol. Sci. & Pol. 107 (2009).

162 *See* Veasey v. Abbott, 830 F.3d 216 (5th Cir. 2016), *cert. denied*, No. 16-393, 2016 WL 5394945 (U.S. Jan. 23, 2017) (Texas law); *McCrory* 831 F.3d at 239 (North Carolina law).

163 *See* Veasey v. Abbott, No. 2:13-cv-00193 (S.D. Tex. Aug. 10, 2016), *available at* https://www.brennancenter.org/sites/default/files/legal-work/2016.08.10_Order-InterimPlan.pdf (establishing alternatives to the Texas photo ID requirements); see *McCrory*, 831 F.3d 204 at 239 (enjoining the North Carolina photo ID requirements.).

164 *See* Frank v. Walker, Nos. 16-3003 & 16-3052, 2016 WL 4224616, at *1 (7th Cir. Aug. 10, 2016), *en banc review denied*, 835 F.3d 649 (7th Cir. 2016) (keeping the ID requirement in place for the November 2016 election.); *see also* One Wisconsin Inst., Inc. v. Thomsen, No. 15-CV-324-JDP, 2016 WL 4250508, at *5-6 (W.D. Wis. Aug. 11, 2016).

165 *See Veasey* 830 F.3d at 265; Veasey v. Abbott, 796 F.3d 487, 493 (5th Cir. 2015), *reh'g en banc granted*, 815 F.3d 958 (5th Cir. 2016); Veasey v. Perry, 71 F. Supp. 3d 627, 659, 698 (S.D. Tex. 2014); Texas v. Holder, 888 F. Supp. 2d 113, 144 (D.D.C. 2012) (finding the Texas photo ID law impermissible under the preclearance provisions of the Voting Rights Act)..

166 *See, e.g.*, Pew Research Center for the People & the Press, Broad Support for Photo ID Voting Requirements 1 (2012), http://www.people-press.org/files/legacy-pdf/10-11-12%20Voter%20ID%20release.pdf.

167 *See, e.g.*, *Administering Michigan's Voter Identification Requirement—Election Day Procedures for Election Inspectors*, State of Michigan, Bureau of Elections–Lansing (2013), https://www.michigan.gov/documents/sos/Photo_ID_Proc_for_Elec_Inspector_212804_7.pdf.

168 La. Stat. Ann. § 18:562.

169 R.I. Gen. Laws §17-19-24.3 (2011).

170 *See generally*, *Veasey* No. 2:13-cv-00193, *available at* https://www.brennancenter.org/sites/default/files/legal-work/2016.08.10_Order-InterimPlan.pdf (allowing voter to present secondary forms of ID). https://www.brennancenter.org/blog/early-voters-texas-dont-have-all-right-information.

171 *See* Myrna Pérez & Jennifer L. Clark, *Early Voters in Texas Don't Have All the Right Information*, Brennan Ctr. for Justice (Oct. 25, 2016).

172 N.H. Rev. Stat. Ann. §659:13(c)(2) (2015).

173 Ed Vogel, *Miller calls for voter photo ID law in Nevada*, Las Vegas Review-Journal (Nov. 27, 2012), http://www.reviewjournal.com/news/elections/miller-calls-voter-photo-id-law-nevada; *see also* Jim Ragsdale, *New technology to be tested at Minnesota electoral polls*, Star Tribune, July 27, 2013, at B1, *available at* http://www.startribune.com/politics/statelocal/217258041.html. Secretary of State Ross Miller's proposal was defeated partly because of the estimated price of implementing these policies. *See* Laura Myers, *NAACP's Vegas confab focuses on voter suppression*, Las Vegas Review-Journal (July 16, 2014), http://www.reviewjournal.com/news/las-vegas/naacp-s-vegas-confab-focuses-voter-suppression. Other reasons include the delays that could be caused by having to take photos at the polls. *See* Ragsdale, *supra*. Moreover, some argue, polling places that serve large populations of people of color and Native Americans would be more likely to experience long lines as a result of this policy because these groups are less likely to have DMV-issued cards. Aura Bogado, *Nevada Led the Country in Expanding the Vote. Now, It's Eyeing Voter ID*, Colorlines (Dec. 3, 2012), http://colorlines.com/archives/2012/12/nevada_democrat_moves_towards_voter_identification_scheme.html.

174 *See e.g.*, Karen Farkas, *Electronic poll books seem conceptually simple but may be vulnerable to hacking and cyber-attacks, experts say*, The Plain Dealer (Mar. 16, 2013), http://www.cleveland.com/cuyahoga-county/index.ssf/2013/03/electronic_poll_books_seem_conceptually_simple_but_may_be_vulnerable_to_hacking_and_cyber_attacks_ex.html; *see also* Jay Weiner, *Voter ID is not the only troublesome issue in Kiffmeyer bill, election groups say*, MinnPost (Feb. 7, 2011), http://www.minnpost.com/politics-policy/2011/02/voter-id-not-only-troublesome-issue-kiffmeyer-bill-election-groups-say. Additional costs may often include training for election officials and poll workers, Internet connection, and maintenance for the machines. *See* Katy Owens Hubler, *All About E-Poll Books*, The Canvass (NCSL, Denver, Colo.), Feb. 2014, at 1, *available at* http://www.ncsl.org/research/elections-and-campaigns/the-canvass-february-2014.aspx#Poll%20Books. Some public officials have pointed out that prices can vary based on the type of hardware used and the rates charged by vendors for software, programming, and management. *See* Telephone Interview by Jennifer L. Clark, Brennan Ctr. for Justice, with Grace Wachlarowicz, Assistant City Clerk, Minneapolis (Aug. 7, 2015). For example, we know of at least one jurisdiction in Minnesota where the e-poll books are made up of iPads, which cost as little as $269 as of the publication of this report. *See* Telephone Interview by Jennifer L. Clark, Brennan Ctr. for Justice, with David Maeda, City Clerk, Minnetonka (Aug. 17, 2015); *see Compare iPad models*, Apple, http://www.apple.com/ipad/compare/ (last visited Dec. 9, 2015).

175 *See, e.g.*, H.B. 3150, 2014 Reg. Sess. (Okla. 2014).

176 Giulia Piccolino, *What other African elections tell us about Nigeria's bet on biometrics*, Wash. Post (Mar. 10, 2015), https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/03/10/what-other-african-elections-tell-us-about-nigerias-bet-on-biometrics/.

177 Razak Ahmad & Sira Habibu, *Election commission may replace ink with biometric system*, AsiaOne (July 19, 2013), http://news.asiaone.com/News/AsiaOne+News/Malaysia/Story/A1Story20130719-438423.html; *see also* Johannes Dell, *Kyrgyzstan's elections: Six things to know,* BBC (Oct. 3, 2015), http://www.bbc.com/news/world-asia-34338715.

178 The Carter Center, Voter Identification Requirements and Public International Law: An Examination of Africa and Latin America 31 (2013), *available at* https://www.cartercenter.org/resources/pdfs/peace/democracy/des/voter-identification-requirements.pdf.

179 *See, e.g.*, Justin Lee, *Gemalto modernizes Guinea's voter register with biometric technology*, Biometric Update (Nov. 24, 2015), http://www.biometricupdate.com/201511/gemalto-modernizes-guineas-voter-register-with-biometric-technology; *see also VOTER REGISTRATION*, Nat'l Election Comm'n Sierra Leone, www.nec-sierraleone.org/Registration.html (last visited Dec. 9, 2015).

180 *See* Jim Wayman, Fed. Election Comm'n, Using Biometric Identification Technologies in the Election Process 1 (2001), *available at* http://www.eac.gov/assets/1/Page/Innovations%20in%20Election%20Administration%2018.pdf.

181 Voter registration drives conducted by non-governmental groups are central to enabling American political participation—especially for underrepresented racial minorities and lower-income persons. *See* Stephen Mortellaro & Michelle Kanter Cohen, Project Vote, Restricting Voter Registration Drives 2 (2014), *available at* www.projectvote.org/wp-content/uploads/2015/06/RESTRICTING-VR-DRIVES-POLICY-PAPER-SEPT-2014.pdf; *see also* Weiser & Norden, *supra* note 154, at 4, 12. Moreover, declines in voter registration drive activity by non-governmental groups has accompanied declines in voter registration rates. *See id.* at 20.

182 Wayman, *supra* note 180, at 10.

183 *See What is Voter Registration*, Republic of Phil. Comm'n on Elections (Aug. 22, 2015), http://www.comelec.gov.ph/?r=VoterRegistration/WhatisVoterRegistration; *see also No Bio, No Boto,* Republic of Phil. Comm'n on Elections (Aug. 22, 2015), http://www.comelec.gov.ph/?r=VoterRegistration/NoBioNoBoto.

184 *Automatic Voter Registration in California,* Brennan Ctr. for Justice (Oct. 12, 2015), https://www.brennancenter.org/analysis/automatic-voter-registration-california.

185 *See, e.g., What is Voter Registration*, *supra* note 183; *see also* Piccolino, *supra* note 176. Biometrics can also have unintended consequences for registered voters without biometric data on file. For example, in the Philippines, the Commission on Elections attempted to prevent voters with existing and active voter registrations from voting unless they effectively "re-registered" by having their biometrics taken. The Supreme Court of the Philippines temporarily halted the Commission's practice ahead of the May 2016 election, but the practice could prevent voters from participating in future elections. *See* Paterno Esmaquel II, *SC stops Comelec from dropping 2.5M voters without biometrics*, Rappler (Dec. 01, 2015, 4:22 PM), www.rappler.com/nation/politics/elections/2016/114575-sc-tro-comelec-biometrics-no-bio-no-boto.

186 Adam Vrankulj*, Kenyans rush to register biometrics ahead of general election, though malfunctions cause delays,* Biometric Update (Dec. 20, 2012), www.biometricupdate.com/201212/kenyans-rush-to-register-biometrics-ahead-of-general-election-though-malfunctions-cause-delays.

187 Adam Vrankulj, *Biometric machines thwart duplicate voters in Ghana presidential election, cause massive delays*, Biometric Update (Dec. 7, 2012), www.biometricupdate.com/201212/biometric-machines-thwart-duplicate-voters-in-ghana-presidential-election-cause-massive-delays.

188 Piccolino, *supra* note 176. While biometrics, in theory, could be captured at the polling place, costs would be much higher due to the need for expensive equipment at every polling place and the need to train technical staff to operate it. *See* Jonathan Bhalla, *Can tech revolutionize African elections?*, CNN (Nov. 17, 2012), http://www.cnn.com/2012/11/17/opinion/sierra-leone-election-biometric/; *see* Alan Gelb & Julia Clark, *Using biometrics in development: lessons and challenges*, The Guardian (Feb. 11, 2013), http://www.theguardian.com/global-development-professionals-network/2013/feb/11/biometrics-development-aid-work.

189 Obviously, people could still be disenfranchised because of uneven or incorrect applications of the photo ID law, or because circumstances are such that the person does not have her accepted ID with her.

190 Some states do not have the trained government employees necessary to properly help voters. For example, the Texas Department of Public Safety, which was tasked with the issuance of Texas' free voter ID cards, did not, as of September 10, 2014, have a single person at the department who was devoted solely to the issuance of the free IDs. Carson Whitelemons, *Texas Photo ID Trial Update: Day Six Afternoon Session*, Brennan Ctr. for Justice (Sept. 10, 2014), https://www.brennancenter.org/blog/texas-photo-id-trial-update-day-six-afternoon-session.

191 A study by the Government Accountability Office reveals that that there are certain costs tied to obtaining the necessary documents needed in order to apply for a free, acceptable voter ID. U.S. Gov't Accountability Office, GAO-14-634, Issues Related to State Voter Identification Laws 28-33 (2014), *available at* http://www.gao.gov/assets/670/665966.pdf. Some of the most costly and time-intensive documents to obtain include underlying documents that are necessary to obtain an acceptable ID. Telephone Interview with Matt Barreto, Professor

of Political Sci., Univ. of Cal. LA (Mar. 3, 2015); *see also* Wendy R. Weiser, *Voter Suppression: How Bad? (Pretty Bad)*, Brennan Ctr. for Justice (Oct. 1, 2014), https://www.brennancenter.org/analysis/voter-suppression-how-bad-pretty-bad.

192 Barreto, *supra* note 191. A sampling of voter ID laws passed during 2011, 2012, and 2013 reveals that not all laws propose or enforce a plan to educate the public about identification requirements. *Voter ID Laws Passed Since 2011*, *supra* note 157. Moreover, the implementation of a system to rovide free IDs does not by itself ensure that voters are aware of identification requirements or of the option to obtain free ID. In Texas, for example, the state had only issued 279 free IDs as of September 2014, two months before Election Day. Manny Fernandez, *Plaintiffs Claim Bias During Closing Argument Against Texas Voter ID Law*, N.Y. Times, Sept. 22, 2014, at A16, *available at* http://www.nytimes.com/2014/09/23/us/plaintiffs-assert-bias-during-closing-argument-against-texas-voter-id-law.html.

193 Atkeson et al., *Who Asks For Voter Identification? Explaining Poll-Worker Discretion*, 76 J. of Pol. 944 (2014), *available at* http://journals.cambridge.org/action/displayAbstract?aid=9342635&fileId=S0022381614000528.

194 *See Shift from Polls to Mail Changes the Way Americans Vote*, News21 (Aug. 12, 2012), http://votingrights.news21.com/article/mail-voting/.

195 Wendy Underhill, *All-Mail Elections (AKA Vote-By Mail)*, Nat'l Conference of State Legislatures (July 7, 2014), http://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx.

196 Voters may vote by mail in all elections in Oregon and Washington. Or. Rev. Stat. § 254.465 (West 2015); Wash. Admin. Code §§ 434-250-37, 120 (2015). While mail voting is the norm in Colorado, certain political subdivisions may conduct elections in person. Colo. Rev. Stat. Ann. § 1-7.5-104 (West 2013); *see also Election Day FAQs*, Colorado Secretary of State, http://www.sos.state.co.us/pubs/elections/FAQs/ElectionDay.html (last visited Dec. 9, 2015).

197 Underhill, *supra* note 195.

198 *Absentee and Early Voting*, Nat'l Conf. of St. Legislatures (Feb. 11, 2015), http://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx.

199 U.S. Election Assistance Comm'n, The 2014 EAC Election Administration and Voting Survey Comprehensive Report 12 (2014), *available at* https://www.eac.gov/assets/1/Page/2014_EAC_EAVS_Comprehensive_Report_508_Compliant.pdf; U.S. Election Assistance Comm'n, 2012 Election Administration and Voting Survey 10 (2013), *available at* https://www.eac.gov/assets/1/Page/990-050%20EAC%20VoterSurvey_508Compliant.pdf.

200 Paul Gronke, Eva Galanes-Rosenbaum, Peter A. Miller & Daniel Toffey, *Convenience Voting*, 11 Ann. Rev. of Pol. Sci., Jan. 2008, 438, 438, *available at* https://www.supportthevoter.gov/files/2013/08/Gronke2008-Convenience_Voting.pdf.

201 *See* Underhill, *supra* note 195.

202 Some studies have concluded that mail ballot systems increase voter turnout. *See, e.g.,* Sean Richey, *Voting by Mail: Turnout and Institutional Reform in Oregon*, 89 Soc. Sci. Q. 902, 902 (2008), *available at* http://www.jstor.org/stable/42956352. In a 2012 study, political scientists

Paul Gronke and Peter Miller concluded that Oregon's vote-by-mail system increased turnout during a short period of time because of its novelty and because of the special circumstances of the years reviewed in that study. Paul Gronke & Peter Miller, *Voting by Mail and Turnout in Oregon: Revisiting Southwell and Burchett*, 40 Am. Pol. Res. 976, 987 (2012). By contrast, a 2007 study of a large sample of voters in California determined that, in general, vote-by-mail elections might actually decrease turnout. Thad Kousser & Megan Mullin, *Does Voting by Mail Increase Participation? Using Matching to Analyze a Natural Experiment*, 15 Pol. Analysis 428, 428 (2007), *available at* http://pages.ucsd.edu/~tkousser/Political%20Analysis-Does%20Voting%20by%20Mail%20Increase%20Turnout_.pdf. Moreover, some studies, such as one conducted in California in 2010, found that a new mail ballot system did not affect turnout even though it prompted some voters to vote in person because of the confusion created when receiving postage-paid envelopes. *See* Melissa R. Michelson et al., *The Effect of Prepaid Postage on Turnout: A Cautionary Tale for Election Administrators*, 11 Election L.J. 279, 279 (2012), *available at* http://www.columbia.edu/~ajc2241/final_stamp.pdf.

203 Adam Liptak, *Error and Fraud at Issue as Absentee Voting Rises*, N.Y. Times, Oct. 6, 2012, at A1, *available at* http://www.nytimes.com/2012/10/07/us/politics/as-more-vote-by-mail-faulty-ballots-could-impact-elections.html?pagewanted=1. Moreover, voters have less confidence that paper absentee ballots are counted than in-person paper ballots cast. R. Michael Alvarez et al., *Are Americans Confident Their Ballots Are Counted?* 70 J. of Pol. 754, 762 (2008), *available at* http://core.ac.uk/download/pdf/4880588.pdf ("Paper absentee ballots and precinct-cast electronic ballots appear to have the largest negative effect on confidence.").

204 U.S. Election Assistance Comm'n 2014, *supra* note 199, at 12.

205 Todd Leopold, *Cyberattack on Florida election raises questions*, CNN (Mar. 18, 2013), http://www.cnn.com/2013/03/18/tech/web/florida-election-cyberattack/. (David Jefferson, a computer scientist, emphasized the significance of this attack, saying, "But because this is the first real documented attack in a U.S. election, it has outsized importance. We can now say we do have an example in a U.S. election of a bona fide cyberattack. You don't have to believe us—we didn't write that grand jury report. Read it." *Id.*) This attack has an interesting historical parallel: the Miami mayoral race in 1997 experienced "significant voter fraud" perpetrated through the absentee balloting system. Demos, Securing the Vote An Analysis of Election Fraud 25 (2003), available at http://www.michiganelectionreformalliance.org/EDR_Securing_the_Vote.pdf. See also *supra* notes 21-24 and accompanying text for further analysis of the 1997 Miami mayoral race.

206 Patricia Mazzei, *Miami-Dade grand jury: Absentee voting fraud clouds confidence in tight election results*, Miami Herald (Dec. 20, 2012), http://www.miamiherald.com/news/politics-government/article1945636.html.

207 Todd Leopold, *Cyberattack on Florida election raises questions*, CNN (Mar. 18, 2013), http://www.cnn.com/2013/03/18/tech/web/florida-election-cyberattack/.

208 *Id.*

209 *Woman sentenced to six months home confinement in voter fraud case*, Brownsville Herald (Apr. 3, 2014, 12:22 PM), http://www.gopusa.com/news/2014/04/03/woman-sentenced-to-six-months-home-confinement-in-voter-fraud-case/.

210 We calculated these numbers using the aforementioned News21 database of cases of alleged voter fraud. *See Exhaustive Database of Voter Fraud Turns Up Scant Evidence That It Happens,*

supra note 26 & accompanying text. We counted all reported absentee ballot fraud cases where the suspect was convicted, pleaded, or in which a consent order was issued. *See Election Fraud in America*, *supra* note 27.

211 Charles Stewart III, *Losing Votes by Mail*, 13 N.Y.U. J. Legis. & Pub. Pol'y 573, 579-81 (2010). Some of the errors causing ballots to be rejected at the end include voters neglecting to sign the ballot or "overvoting," in other words accidentally voting for more than one candidate for the same contest. *See id.* at 591. A study of the mail absentee ballot system in California noted that the most likely reason a mail ballot was rejected was that it was received after the close of the polls. R. Michael Alvarez et al., *Whose absentee votes are returned and counted: The variety and use of absentee ballots in California*, 27 Electoral Stud. 673, 676 (2008), *available at* https://pages.wustl.edu/betsysinclair/r.-michael-alvarez-thad-e.-hall-and-betsy-sinclair.-2008.-whose-absentee-votes-are.

212 Stewart, *supra* note 211, at 581. Washington state has tried to address the problem of lost ballots in the pipeline in a variety of ways, including: creating in-person drop boxes for returning ballots (which provide an alternative to the U.S. post office); allowing voters to check online to see if their ballot was received; and allowing voters to log in and access an electronic replacement ballots for printing and return if the voter does not receive her ballot or makes a mistake. E-mail from Lori Augino, Dir. of Elections, Wash. Office of the Sec'y of State, to author (Sept. 16, 2015 14:32 EST) (on file with author).

213 *See generally* Stewart, *supra* note 211. The EAC's Election Management Guide recommends ways for election officials to ward against security concerns during a number of checkpoints during the vote-by-mail process. These include tracking the number of ballots mailed to voters, ensuring that secure drop sites are used, and planning an organized way of sorting ballots. *See* Election Assistance Comm'n, *Absentee Voting and Vote By Mail*, *in* Election Management Guidelines 51-59 (Election Assistance Comm'n, ed., 2010), *available at* http://www.eac.gov/assets/1/workflow_staging/Page/264.PDF. A convening of experts would allow for greater detail in identifying the types of concerns on which officials should concentrate their efforts.

214 In Washington, even though all voters are mailed a vote-by-mail ballot, there are some elections in which the majority of voters are using one of the vote by mail drop boxes to return their ballot. Augino, *supra* note 212.

215 *See Most Frequently Asked Questions*, *Elections and Voting*, Office of the Sec'y of State, https://wei.sos.wa.gov/agency/osos/vi/pages/ballotsecrecy.aspx (last visited Dec. 9, 2015); Colo. Rev. Stat. § 1-7.5-207 (2013); *see* Ballot Track, Arapahoe County Elections, http://www.arapahoevotes.com/ballot-track/ (last visited Dec. 9, 2015); Jefferson Dodge, *Can Your Vote be Traced?*, Boulder Wkly. (Sept. 6, 2012), http://www.boulderweekly.com/article-9651-can-your-vote-be-traced.html; Allison Terry, *Voter turnout: the 6 states that rank highest, and why*, Christian Sci. Monitor (Nov. 6, 2012), http://www.csmonitor.com/USA/Elections/2012/1106/Voter-turnout-the-6-states-that-rank-highest-and-why/Oregon.

216 Patrick, *supra* note 50. Seth Flaxman, Founder and Director of Democracy Works, also testified and submitted written materials to the PCEA on the benefits of IMB. *See* Testimony of Seth Flaxman, Presidential Comm'n on Election Admin. 80-81 (Sept. 4, 2013), https://www.supportthevoter.gov/files/2013/11/PCEA-Philadelphia-Public-Meeting-Transcript.pdf; Memorandum from Seth Flaxman et al. to the Presidential Comm'n on Election Admin. 7 (Nov. 6, 2013), *available at* https://www.supportthevoter.gov/files/2013/11/Vote-by-Mail-Reform-Memo.pdf.

217 Wash. Rev. Code § 29A.40.110(3) (2012); Dan Frosch, *Colorado Mail-In Voting Gets Early Test—New Statewide System Will Be Used on Closely Watched Races*, Wall Street J. (Nov. 3, 2014), *available at* http://www.wsj.com/articles/colorado-mail-in-voting-gets-early-test-1415049406; Associated Press, *13,000 Oregon ballots rejected for signature issue*, Wash. Times (Nov. 11, 2014), *available at* http://www.washingtontimes.com/news/2014/nov/11/13000-oregon-ballots-rejected-for-signature-issue/.

218 Or. Sec'y of State, Vote by Mail Procedures Manual 28 (2014), *available at* http://sos.oregon.gov/elections/documents/vbm_manual.pdf.

219 Wash. Rev. Code § 29A.40.110(3) (2012).

220 Telephone Interview with Lori Augino, Dir. Of Elections, Office of Sec'y of State of Wash. (Mar. 28, 2015).

221 Frosch, *supra* note 217.

222 Lorraine C. Minnite, The Myth of Voter Fraud 29 (2010). Dr. Minnite lists these, and other types of election fraud, noting that "[a]ll states have prohibitions against falsifying voter registration information, voting more than once in an election, impersonating another voter, intimidating or coercing voters, and bribing voters or buying votes." *Id.*

223 52 U.S.C. §10308(a) (2012 & West Supp. 2015).

224 *See* Soumya Karlamangla, *Alarcon conviction is the latest in string of residency prosecutions*, L.A. Times (July 24, 2014, 6:43 PM), http://www.latimes.com/local/la-me-adv-alarcon-prosecution-20140725-story.html.

225 *See* Press Release, U.S. Attorney's Office, S. Dist. of W. Va., Former Chief Magistrate of Mingo County Pleads Guilty to Federal Election Fraud (Dec. 2, 2013), *available at* http://www.fbi.gov/pittsburgh/press-releases/2013/former-chief-magistrate-of-mingo-county-pleads-guilty-to-federal-election-fraud.

226 *See* Press Release, U.S. Attorney's Office, Dist. of Mass., Massachusetts State Representative Stephen Smith Agrees to Plead Guilty to Voter Fraud Charges (Dec. 20, 2012), *available at* http://www.fbi.gov/boston/press-releases/2012/massachusetts-state-representative-stephen-smith-agrees-to-plead-guilty-to-voter-fraud-charges.

227 Kimball Perry, *Ohioan gets 5-year prison term for illegal voting*, USA Today (July 17, 2013, 6:16 PM), http://www.usatoday.com/story/news/nation/2013/07/17/cincinnati-illegal-voting/2530119/.

228 Corey Dade, *Indiana's Top Election Official Convicted of Voter Fraud,* NPR (Feb. 6, 2012, 3:19 PM), http://www.npr.org/sections/itsallpolitics/2012/02/06/146473653/indianas-top-election-official-convicted-of-voter-fraud.

229 Research indicates that long-serving managers or directors are the most susceptible to the opportunities and pressures that lead someone to commit fraud. Telephone Interview with Steve Albrecht, Professor, Marriot Sch. of Mgmt., Brigham Young Univ. (Mar. 18, 2015).

230 *Id.*

231 Telephone Interview with James D. Ratley, President, Ass'n of Certified Fraud Exam'rs (Mar. 10, 2015).

232 *Id*.; Albrecht, *supra* note 229.

233 Albrecht, *supra* note 229. Analogues would include setting limits on who was authorized to make revisions to the statewide voter registration database, designating certain people to review signature authenticity, and maintaining control over absentee and provisional ballots.

234 There is general agreement that risk of detection within the private sector serves as a strong deterrent to would-be criminals. *See* Lawrence Bader, *Is the Current Wave of Insider Trading Cases a Deterrent to Others?*, Forbes (Dec. 12, 2012), http://www.forbes.com/sites/insider/2012/12/12/is-the-current-wave-of-insider-trading-cases-a-deterrent-to-others/; *see also* James B. Stewart, *In a New Era of Insider Trading, It's Risk vs. Reward Squared*, N.Y. Times, Dec. 8, 2012, at A1, *available at* http://www.nytimes.com/2012/12/08/business/insider-trading-persists-and-gets-stealthier.html ("It's still too soon to measure the deterrent effect of the latest wave of [securities laws enforcement] cases, but it's surely substantial.").

235 *See* Albrecht, *supra* note 229; Brennan Ctr. for Justice, Testimony of the Brennan Center for Justice at NYU School of Law, Presidential Comm'n on Election Admin. 27 (Sept. 4, 2013), https://www.supportthevoter.gov/files/2013/11/Testimony-of-the-Brennan-Center-for-Justice-before-the-PCEA.pdf.

236 Ratley, *supra* note 231.

237 Ass'n of Certified Fraud Exam'rs, Report to the Nations on Occupational Fraud and Abuse 40 (2012), *available at* http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf.

238 *See Stop Voter Fraud*, Ga. Sec'y of State, http://sos.ga.gov/index.php/elections/stop_voter_fraud (last visited Dec. 9, 2015); *Elections Fraud Complaint*, Fla. Div. of Elections, http://dos.myflorida.com/elections/contacts/elections-fraud-complaint/ (last visited Dec. 9, 2015); *Elections Compliance Unit*, La. Sec'y of State, http://www.sos.la.gov/ElectionsAndVoting/GetInvolved/ReportElectionFraud/Pages/default.aspx (last visited Dec. 9, 2015).

239 Ratley, *supra* note 231.

240 Kim Nilsen, *Keeping Fraud in the Cross Hairs*, J. of Acct., June 1, 2010, *available at* http://www.journalofaccountancy.com/issues/2010/jun/20102852.html (see "Fraud Prevention Checklist"). According to James D. Ratley, CFE, "Punishment has to be swift and sure, and [workers] need to know that there are consequences." Ratley, *supra* note 231.

241 Albrecht, *supra* note 229.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at **www.brennancenter.org.**
Sign up for our electronic newsletters at **www.brennancenter.org/signup.**

Latest News | Up-to-the-minute information on our work, publications, events, and more.

Justice Update | Snapshot of our justice work and latest developments in the field.

Fair Courts | Comprehensive news roundup spotlighting judges and the courts.

Redistricting Round-Up | Analysis of current legal battles and legislative efforts.

Liberty & National Security | Updates on privacy, government oversight, and accountability.

Twitter | www.twitter.com/BrennanCenter
Facebook | www.facebook.com/BrennanCenter
Instagram | www.instagram.com/BrennanCenter

NEW AND FORTHCOMING BRENNAN CENTER PUBLICATIONS

The Justice Department's Voter Fraud Scandal: Lessons
Adam Gitlin and Wendy Weiser

Florida: An Outlier in Denying Voting Rights
Erika Wood

The Fight to Vote
Michael Waldman

America's Voting Machines at Risk
Lawrence Norden and Christopher Famighetti

The Case for Automatic Voter Registration
Brennan Center for Justice

Stronger Parties, Stronger Democracy: Rethinking Reform
Ian Vandewalker and Daniel I. Weiner

How Many Americans are Unnecessarily Incarcerated?
Dr. James Austin and Lauren-Brooke Eisen with James Cullen and Jonathan Frank

The New Era of Secret Law
Elizabeth Goitein

For more information, please visit **www.brennancenter.org.**

BRENNAN CENTER
FOR JUSTICE
TWENTY YEARS

at New York University School of Law

120 Broadway
Suite 1750
New York, NY 10271
646-292-8310
www.brennancenter.org