ELECTION INTEGRITY: A PRO-VOTER AGENDA

By Myrna Pérez

BRENNAN CENTER
FOR JUSTICE
TWENTY YEARS

at New York University School of Law

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]