



***IS THIS  
ANY WAY  
TO VOTE?***



***VULNERABLE  
VOTING MACHINES  
AND THE  
MYSTERIOUS  
INDUSTRY  
BEHIND THEM***

**PLUS: IS MAIL-IN VOTING THE ANSWER?**

**CELESTE KATZ MARSTON AND GABRIELLA NOVELLO**

Presented by **WHO.WHAT.WHY.**

# IS THIS ANY WAY TO VOTE?

Vulnerable Voting Machines and the  
Mysterious Industry Behind Them

CELESTE KATZ MARSTON AND GABRIELLA NOVELLO

WhoWhatWhy  
New York City

Copyright © 2020 by WhoWhatWhy

All rights reserved. No part of this book may be used or reproduced in any manner whatsoever without written permission from the publisher, except in the case of brief quotations embodied in critical articles and reviews.

Cover design by Cari Schmoock. Cover art and photo editing by Michael Samuels. Data visualizations by Lizzy Alves.

Published in the United States by WhoWhatWhy.  
eBook ISBN 978-1-7329219-1-7

WhoWhatWhy® is a registered trademark of Real News Project, Inc.

# CONTENTS

<a href="#">Initialisms and Acronyms Used in This Book</a>	vi
<a href="#">Introduction</a>	1
1. <a href="#">The Voting-Machine Manufacturers</a>	5
2. <a href="#">The Voting Machines</a>	25
3. <a href="#">Voting Machine Accessibility</a>	42
4. <a href="#">Voting Machine Vulnerabilities</a>	55
5. <a href="#">Solutions and Global Perspectives</a>	77
6. <a href="#">Conclusion</a>	102
7. <a href="#">Addendum: Is Mail-in Voting the Answer?</a>	108
 <a href="#">About the Authors</a>	 116
<a href="#">About WhoWhatWhy</a>	118
<a href="#">Glossary</a>	119



# INITIALISMS AND ACRONYMS USED IN THIS BOOK

---

**ADA** Americans with Disabilities Act  
**BMD** ballot-marking device  
**COIB** Conflicts of Interest Board  
**DRE** direct-recording electronic machine  
**EAC** Election Assistance Commission  
**EMS** election management system  
**ES&S** Election Systems & Software  
**FVAP** Federal Voting Assistance Program  
**FWAB** Federal Write-In Absentee Ballot  
**HAVA** Help America Vote Act  
**MPSA** Military Postal System Agency  
**NPRM** notice of proposed rulemaking  
**OSET** Open Source Election Technology Institute  
**RFP** request for proposal  
**RLA** risk-limiting audit  
**SQL** Structure Query Language  
**TGDC** Technical Guidelines Development Committee  
**UOCAVA** Uniformed and Overseas Citizens Absentee Voting Act  
**VSAP** Voting Solutions for All People  
**VVPAT** Voter Verified Paper Audit Trail  
**VVSG** Voluntary Voting System Guidelines



Photo credit: [Florida Memory / Flickr](#)

When we talk about elections, we often focus on the campaign horserace, who is up or down in the polls, the back and forth between candidates, and maybe a little about which issues matter most to voters. Sometimes there's even a little discussion about rules that have denied voting rights for hundreds of thousands of Americans of color.

What we rarely talk about is *how* we vote.

This e-book focuses on a few fundamental questions: How secure and reliable are the machines we use to vote? How do they work? How do our public officials choose which ones to buy?

For election results to be believable, the system needs to be clearly understandable to everyone. The credibility of American democracy depends on it.

Most Americans are familiar with the companies that make their cars, laptops, and cell phones. These companies are constantly scrutinized, and when something goes wrong — an airbag fails to open or a laptop or cell phone battery overheats and catches fire — everyone knows about it. But how many people can say who makes their **voting machines** or how dependable they are?

In these pages, *WhoWhatWhy* asks and answers the big questions concerning the “Big Three” manufacturers that produce the machines that will be used to decide the 2020 elections. The companies are Election Systems & Software (ES&S), Dominion, and Hart InterCivic. We will look at some of the advantages and vulnerabilities inherent in their systems.

Most of our reporting has been carried out with the aid of experts from across the nation. There has been remarkably little assistance from the companies themselves. ES&S, by far the largest of the

three, boasts that its motto is to “talk straight and communicate openly and honestly with others and ourselves.”<sup>1</sup> The company, nevertheless, declined to make any representative available to answer the questions raised in this book. Dominion and Hart InterCivic didn’t even bother to respond to requests for comment.

This book explores the nuts and bolts of how we vote in America and where our basic election infrastructure is vulnerable. We suggest this system can be improved by investing in better technology, supporting a more transparent procurement process, and enacting legislation to regulate smarter voting procedures. We also look at lessons learned from election processes — both good and bad — in other nations.

Finally, we explore the push for increased mail-in voting and the direction voting is likely to take once the 2020 election and the COVID-19 pandemic have passed into history.

In times of political passion, Americans can be expected to make their voices heard through this bedrock act of our democracy. And yet, the COVID-19 pandemic has upended that fundamental expression: It has forced a number of states to postpone primary elections. It has laid land mines in the path of campaigns and surrogates. And with the US economy teetering from the pandemic shutdowns, it has cut into spending on crucial election measures (such as increased staffing to handle the rise of absentee voting) and the security steps<sup>2</sup> that are supposed to guarantee a fair vote for everyone.

Despite the challenges, federal law and the Constitution itself mandate the 2020 presidential election must go on.

## Notes

1. "[Company Overview](#)," Election Systems & Software, accessed April 19, 2020.
2. Matthew Vann, "[Some cash-strapped states turn to election security funds to fight COVID-19](#)," ABC News, April 6, 2020.

1.

# THE VOTING-MACHINE MANUFACTURERS

---

## *Who are the Big Three?*

### **Election Systems & Software (ES&S)**

By far the dominant supplier of voting equipment in the United States is Election Systems & Software, better known by its initials, ES&S. Headquartered on John Galt Boulevard<sup>1</sup> in Omaha, NE, ES&S makes machines that are used in elections throughout the country. As a private company, it is not required to disclose its finances or inner workings.

On its website, ES&S states that it provides a wide array of services before, during, and after elections, including registering voters, printing ballots, training poll workers, tabulating and reporting results, auditing, and recounting. *ProPublica* reported in 2019 that ES&S controlled around 50 percent of the market.<sup>2</sup> In the past several years, ES&S has highlighted its presence in places including Pennsylvania, South Carolina, North Carolina, Delaware, and Wyoming.<sup>3</sup>

According to ES&S's website, the company is owned by individual members of ES&S management and by the McCarthy Group.



A letter written in 2019 by ES&S Vice President of Finance Richard Jablonski to the North Carolina State Board of Elections and Ethics Enforcement sheds a little more light on the ownership. It states that “Government Systems, Software & Services, Inc. (GSS&S) owns 100% of the membership units of Election Systems & Software, LLC” and that five percent or more of the shares in GSS&S belong to the McCarthy Group LLC.<sup>4</sup> (The letter, made public by the Florida Fair Elections Coalition, says the company considers the names of anyone with substantial ownership interest to be “proprietary and confidential information.”)

The McCarthy Group, which is also headquartered in Omaha, says on its website that it “manages more than \$1.5 billion of capital.”<sup>5</sup>

In 2009, ES&S acquired Premier Election Solutions, the division of Diebold that manufactures voting machines. At the time, *Wired* reported that ES&S systems were already used “in counting approximately 50 percent of the votes in the last four major U.S. elections.”<sup>6</sup> This means ES&S has been the main player for more than a decade.

In 2010, the Justice Department ordered ES&S to divest from Premier Election Solutions, Inc. “in order to restore competition.” The merger had “combined the two largest systems providers used to tally votes in federal, state and local elections in the United States.”<sup>7</sup>

Dominion Voting Systems finally bought the Premier assets that ES&S was forced to sell.<sup>8</sup>

## **Dominion Voting Systems**

Dominion Voting Systems claims to have been around for more than a century, “with roots all the way back to 1895 and the invention of the first ever Direct Recording lever machines in New York.”<sup>9</sup>

The company has international headquarters in Toronto and its US headquarters in Denver. It counts many counties in New York State among its clients, as well as having a presence in Illinois, Nevada, and Louisiana, as well as in Canada, Mongolia, and the Philippines.<sup>10</sup>

A profile assembled by Dun & Bradstreet describes Dominion as making

specialized hardware and software used by some 600 US jurisdictions in 22 states, as well as by jurisdictions in Canada and other countries. Its flagship product line, Democracy Suite, comprises various systems used by election officials, including optical ballot scanners and vote tabulators, voter list generators, election management software, and electronic ballot systems for absentee voting.<sup>11</sup>

In addition to buying Diebold’s Premier Election Systems, Dominion bought another voting supply company, Sequoia.<sup>12</sup>

After Florida’s infamous “hanging chad” controversy during the 2000 presidential election, which led to challenges going all the way to the US Supreme Court, Dan Rather raised serious questions about Sequoia.<sup>13</sup> The company had produced the punch cards that had failed Florida voters. *Wired* reported:

Rather and his producers spoke with several former workers of Sequoia who revealed that in 2000 the company changed

the paper stock it used for punch cards [and] that they knew before the election that the punch cards that Sequoia was producing would cause problems.<sup>14</sup>

In 2019, the company found itself the target of activists' concerns after the state of Georgia contracted to use its Dominion ImageCast X Voting System, which *WhoWhatWhy* describes as

a type of ballot-marking device [that] allows voters to mark a ballot on paper or electronically, but produces a summary count of votes on a **QR code** rather than a human-readable paper list.<sup>15</sup>

Unlike conventional paper lists, the QR codes can't be read by poll workers, and can only be tallied by Dominion's machines.

### **Hart InterCivic**

Hart InterCivic, headquartered in Austin, TX, with regional offices in California, Hawaii, Idaho, Illinois, Michigan, and North Carolina, offers a wide range of services, which according to its Bloomberg company profile includes paper ballots, precinct digital scans, electronic poll books, election night reporting, supplies, and printed ballot products.<sup>16</sup> Hart does business in places including Tennessee, Texas, California, Missouri, Idaho, and Oregon.<sup>17</sup>

With a large stake in the company controlled by H.I.G. Capital, a self-described "leading global private equity investment firm with \$37 billion of equity capital under management,"<sup>18</sup> Hart, who did not respond to repeated requests for an interview, is also no stranger to controversy.

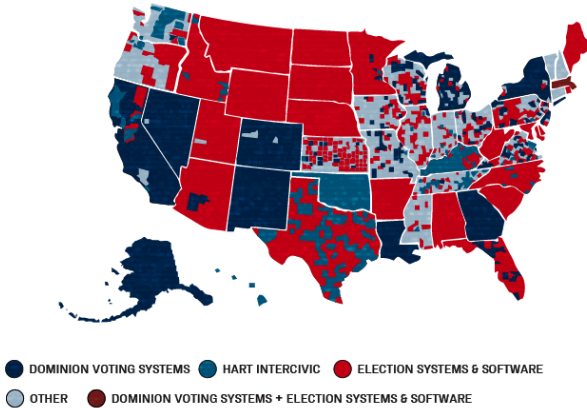
During the 2018 midterms, for example, a number of "straight-ticket" voters complained that Hart's eSlate system had switched

their choices to the opposite party. The complaints to the Texas secretary of state's office recalled similar complaints that had cropped up in Texas a decade earlier.<sup>19</sup>

Like its competitors ES&S and Dominion, Hart is a privately held company and is not required to release detailed financial and operational information to the public. Of the Big Three manufacturers, Hart InterCivic has the smallest market share.<sup>20</sup>

### **ELECTION SYSTEMS & SOFTWARE, DOMINION VOTING SYSTEMS, OR HART INTERCIVIC?**

Which of these companies operate in which states?



Source: <https://www.verifiedvoting.org/verifier/>

### ***Who are the other players in the market?***

Aside from the Big Three, a number of other vendors compete for considerably smaller slices of the market for voting hardware and software.

Voatz, founded in 2015 by two people who won a SXSW hackathon, is a mobile elections platform designed to leverage “smartphone technology with biometrics and blockchain technology in order to make voting more accessible” and discourage voter coercion.<sup>21</sup> The app works on an iPhone 5s or later, and on Android phones dating from 2016 or later. The company claims its app has been used in “more than 30 successful live elections that range from state party conventions [to] student government elections” and voting at town meetings. The largest vote using the app involved more than 15,000 votes. Voatz has been used in pilot programs in Colorado, Utah, and West Virginia. A recent study by MIT identified potential vulnerabilities in the app.<sup>22</sup>

Shadow Inc., now called BlueLink, produced an app called IowaReporter, which met with disastrous results in the 2020 Iowa caucuses. The Iowa Democratic Party contracted with Shadow, a for-profit startup owned by the nonprofit activist group ACRONYM, which has ties to former aides to the Obama administration and Hillary Clinton’s presidential campaign. It was used to report the results of the Iowa presidential caucuses, but after it malfunctioned the Democratic National Committee announced it had decided not use the app in Nevada or other primaries. The Iowa Democrats said the app’s malfunction was due to technical problems, not outside hacking or meddling.<sup>23</sup>

Smartmatic claims to have “helped hundreds of millions of voters cast over 4 billion votes in thousands of elections around the world.”<sup>24</sup> With its world headquarters in London and US offices in Florida and California, the company worked with Los Angeles County on a new election system dubbed “Voting Solutions for All People,” or VSAP, which was “built with open-source technology over 10 years for \$100 million [total costs came closer to \$300 million], and combined with a rethink of the voting process that

lets local voters cast ballots over 11 days instead of 13 hours.”<sup>25</sup> A combination of high turnout in the county’s primary and glitches with the new system, not to mention the deployment of 22,000 machines, resulted in delays and frustration among voters who tested their new setup. As with other systems, Smartmatic had also been flagged early on with security concerns preceding its debut.<sup>26</sup>

### *Why a virtual monopoly?*

For a system directly used by so many people — nearly 137 million Americans voted in 2016 and more than 122 million voted in 2018<sup>27</sup> — it might be surprising that there are not more players in the election equipment business.

Unlike in other places, elections in the United States — even national ones — are not solely controlled by the federal government. There is a complex patchwork of laws that differ between states, counties, major cities, and even villages and towns. Each can have their own rules and purchase their own hardware and software with their own specifications.

Arguably, this setup speaks to the American tradition of rejecting centralized control of major functions and institutions. Some advocates of the current patchwork system say local control of elections makes it “very difficult to steal or manipulate an election in the U.S.”<sup>28</sup> Any irregularity in election results is a serious concern, but they argue the patchwork makes it harder to tamper in a wholesale way with the outcome of, say, a race for president. However, others point out that the patchwork system can contain vulnerabilities to interference that might not exist in a more evenly regulated system. And with the Electoral College, those who want to



interfere might only need to alter results in a few places to change the outcome of a presidential election.

### *Why so few?*

A tiny group of companies have become dominant in the field of voting equipment, in part because they are deeply engaged in setting up the rules that govern who can enter the marketplace.

Tammy Patrick, senior adviser to the Democracy Fund, a bipartisan foundation that promotes advances in election administration, says it's been feast or famine for the companies that produce the machines.

Before the 2000 elections, most vendors sold equipment on a rolling basis as districts replaced aging machines. "One year they were in Nebraska," said Patrick, "the next year it might be Minnesota." In the wake of the controversy surrounding the 2000 presidential elections, however, Congress passed the **Help America Vote Act** (HAVA),<sup>29</sup> which created new election standards to help prevent meltdowns similar to the one that plagued Florida. With the changed requirements, election commissions across the United States were suddenly forced to buy new voting equipment at roughly the same time. That resulted in a temporary sales bonanza. Once the sudden demand had been met, however, sales numbers dropped and remained stagnant for nearly a decade.<sup>30</sup>

"That's a huge shift in a market," said Patrick. Smaller vendors either dropped out of the market completely, or were taken over by the bigger players.

The market for new voting machines is relatively small — about \$300 million<sup>31</sup> — “and it’s highly regulated, and there aren’t very many opportunities to sell new equipment. So for new companies, it’s really not a great business to get into,” said Ben Adida, executive director of Voting Works, a nonpartisan nonprofit that makes machines and software to conduct and audit elections.

By law, when the government begins to set new regulations regarding elections and to define the hardware and software used to conduct them, it is required to make a “notice of proposed rulemaking,” or NPRM, available to the public. Even though the changes may have a profound effect on elections, the average citizen usually shows little or no interest.

Gregory Miller, CEO and co-founder of the Open Source Election Technology Institute (OSET), points out that while the process passes over the heads of most citizens, it is intensely followed by the commercial interests, vendors, and others who have a stake in the outcome of how regulations governing the purchase of election equipment are written. They hire lawyers and lobbyists, overwhelming everyone at the table during what Miller described as a “sausage-making exercise.”

During the last proposed rulemaking process “the largest spenders came in with their lobbyists,” said Miller, “and they essentially helped craft the regulations that are known today as the HAVA regulations.” It was obvious, at least to Miller, that the lobbyists would make certain that the new rules served their company interests.

Reinstating a monopoly was an obvious goal. “They create[d] barriers to entry,” said Miller. Mostly, this was accomplished by creating high “switching costs,” which meant each player was almost guaranteed to keep its customer base.

Miller compares the setup to the one the Food and Drug Administration uses when approving new medicines. “A perfect example of a ‘barrier to entry,’” Miller said, “is to institute a federal certification program.” That alone can become “incredibly costly,” he said. Developers need enormous amounts of cash if they want to even begin to break into the marketplace.

Proprietary data formats, Miller explains, can also provide a strategic way to lock government agencies into a company’s system, especially when systems manufactured by different companies need to interact with each other.

Miller said that if you run elections in a state, and you want to switch systems, “you’re going to have to figure out how to take all of that data and either reverse engineer it or rewrite it.”

Bottom line: Building a relatively impregnable, affordable, easy-to-use voting machine is difficult, and the companies who have already cornered that market are not anxious to share the wealth.

### ***How should the procurement process work?***

States and municipalities have their own policies for choosing voting systems and the equipment to operate them. Some states require contracts to go to the lowest qualified bidder for everything required. Transparency rules would give the public and bidders a chance to see the proposals that are submitted.

Regulations concerning possible conflicts of interest would keep officials from voting on bids by any company in which they have a personal financial stake or which employs a close relative.

The federal Election Assistance Commission (EAC) does provide numerous resources specifically designed to help government bodies run a fair, smooth, and effective procurement and implementation process.

For example, the commission advises issuing a draft request for proposal (RFP) before publishing a formal RFP. This ensures that bidders on a contract have time to evaluate the draft and provide feedback and that any modifications resulting from bidder feedback do not favor an individual bidder or group of bidders.<sup>32</sup>

The commission also suggests establishing a special website that can serve as a central hub for everything having to do with the RFP. That could include information on what the locality hopes to buy, a Plan B to use if no bidder meets the requirements, records of bid-related meetings, and security procedures for protecting proprietary details.

In addition, the commission suggests that when procuring voting systems, purchasers should “determine if security and functional updates will be included in the contract, or software license, and who will be responsible for implementation of the updates.”<sup>33</sup>

They also should consider whether machines are compatible with locally mandated options, such as ranked-choice and straight-ticket voting, as well as how the machines interact with voter registration databases and electronic poll books (which election workers use to look people up and confirm that they are qualified to vote),<sup>34</sup> and whether it is better to lease equipment or buy it outright.

### ***What are the flaws in the process?***

Philadelphia's purchase of new voting equipment provides a classic example of a procurement process gone bad.

In late 2019, the *Philadelphia Inquirer* reported a sordid story concerning a vendor who had managed to win a \$29 million contract to supply the city with new voting machines.<sup>35</sup> The sale followed a year-long effort to lobby election officials, who unsurprisingly had rushed through an opaque process that was ultimately revealed to be biased in favor of the manufacturer who had spent heavily on lobbying.

Normally, Philadelphia commissioners have the authority to rule on contracts pertaining to the city voting system. The system is supposed to work on a "best value" proposition. If there is a reasonable justification, the city can sign a contract with a company that may not have offered the lowest bid — as long as there is an advantage in quality or design that makes the extra expense worthwhile. After an investigation, City Controller Rebecca Rhynhart found serious problems with the way three city commissioners made their decision to buy a new voting system from ES&S.<sup>36</sup>

"We found a lot of issues," Rhynhart told *WhoWhatWhy*.

While the Pennsylvania Department of State directed several counties to procure **electronic voting** systems by the end of 2019,<sup>37</sup> Rhynhart's office discovered that ES&S had already been involved with the city commissioners as early as 2013, when one commissioner visited the company's headquarters.

That turned out to be the only visit by any commissioner to a potential election equipment vendor.

The commissioner, Al Schmidt, had received at least two campaign contributions from a lobbying firm employed by ES&S that year — one before the visit and one afterward, according to Rhynhart's report. Additionally, by the time of the controller's report, Rhynhart learned that ES&S had spent more than \$425,000 lobbying the City of Philadelphia, "including \$27,856" related to the commissioner who had visited the voting-machine manufacturer's headquarters.

Rhynhart also discovered that ES&S failed to disclose that its lobbying firms, Duane Morris and Triad Strategies, had made campaign contributions in 2017 and 2018 to two commissioners involved in awarding the voting machine contract.

Rhynhart said the lack of disclosure was worrisome enough to justify immediately reporting it to the city's law department. Despite concerns, she said, the city, represented by the mayor and the city commissioner, decided to let ES&S off the hook but required the company to pay a penalty of \$2.9 million. The fine, the biggest in Philadelphia history, constituted 10 percent of the contract's value. The city then decided to stick with ES&S instead of voiding the contract.

Philadelphia ultimately bought the ES&S ExpressVote XL touchscreen system and used it for its November 2019 elections. The system eventually became the subject of a lawsuit over decertification for use.<sup>38</sup>

Asked if Philadelphia's experience might serve as a cautionary tale about procurement, Rhynhart says others could look to the worrisome findings — such as the failure to disclose campaign contributions, and favoritism toward a single vendor — to provide guidance for the future.



Looking back, Rhynhart says the principal question the investigation failed to answer was: Why was the determination to choose ES&S's machines so intense? ES&S's machines were more expensive than the competition, and there was no clear reason for choosing ES&S technology over the competition. "And then," she said, "we found all these things that were wrong. We found the procurement process wasn't followed. We found it was opaque. We found that there was favoritism towards one vendor. You know, we found so many things. I mean, [it] was horribly flawed."

At the time, Commissioner Lisa Deeley objected to the report, insisting in an interview with the *Philadelphia Inquirer* that the allegations were "ridiculous," and stressing that as far as she was concerned there was no conflict of interest. "I did my job, to the fullest of my ability with complete integrity," she told the *Inquirer*.<sup>39</sup>

Oregon Sen. Ron Wyden doesn't mince words when it comes to the sales tactics of the Big Three.

"The lobbyists for ES&S and the other big election technology companies have been selling snake oil to state and election officials, saddling them with overpriced, insecure junk," Wyden told *WhoWhatWhy*.

"There are all kinds of stories in the news about company officials wine-ing and dining election officials," explained Wyden, a Democrat who is outspoken when it comes to voting infrastructure issues. "In Georgia, one of the top ES&S lobbyists even went to work for the governor," he said, referring to Charles Harper, a former ES&S lobbyist, who was picked by Georgia Republican Gov. Brian Kemp to be a top aide.<sup>40</sup>

Wyden says that buying expensive, unsecure election machines guarantees long lines on election day and sizable profits for the

companies who sign states up to long-term maintenance contracts. The computerized machines also provide an entry point for hostile foreign governments to influence election outcomes by hacking into the systems.

### ***What happens when a voting machine company pulls out all the stops to keep a client?***

Greg Gordon, an experienced investigative reporter for the McClatchy newspaper chain, led a team looking into how ES&S had courted election officials over a number of years.

In an extensive report published in 2018, Gordon's team found that ES&S had enticed state and local election officials to serve on an "advisory board" for nearly a decade. The "board" gathered twice a year for company-sponsored events at luxurious locations, including an expensive Las Vegas resort hotel.<sup>41</sup>

It was obvious from Gordon's report that the elbow-rubbing risked compromising the decisions made by these officials, or at least the way in which those decisions were likely to be perceived. The extent of the impropriety became more serious when it became clear that Russia and other nations such as Iran and China were reportedly exploring the possibility of using computer hacking to disrupt the 2018 midterm elections.<sup>42</sup>

Election watchdogs, the McClatchy investigation noted, frequently identify "hospitality and hobnobbing" between vendors and election officials as a glaring problem. For their part, ES&S representatives insist the company's tactics have not compromised the process. Government employees, they explain, had traveled to the meetings

at government expense, with taxpayers, not ES&S, picking up the tab.

There are certainly exceptions to that assertion. One example: In spring of 2020, the executive director of the New York City Board of Elections, Michael Ryan, agreed to pay a fine of \$2,500 to the city Conflicts of Interest Board (COIB) after allowing ES&S to pay his bill for a two-night stay at the Marriott Marquis hotel in Manhattan.<sup>43</sup> Ryan, an unpaid member of an ES&S “advisory board,” lives elsewhere in the city but said he stayed at the hotel because he “socialized” with other board members the night before making a presentation to the group. COIB issued the fine because in accepting the hotel stay, Ryan ran afoul of a prohibition on accepting “any valuable gift” from a company that does business with the city — in this case, of course, that being New York’s voting-machine vendor.

Gordon told *WhoWhatWhy* his investigation disclosed that practices in voting machine purchasing mirror the cozy relationships that characterize procurement and lobbying in general.

“They’re constantly wooing or courting the people in office,” Gordon said, “so it’s not a big surprise that they would set up an ‘advisory committee.’” The cover, Gordon said, enables the company to wine and dine officials at fun, far-flung events. “I don’t think anybody would leap at a chance to go to Omaha [ES&S’s headquarters],” Gordon explained.

The officials involved clearly saw no problem in accepting free meals, drinks, travel, or entertainment. Gordon said most convinced themselves that the gifts didn’t really count and they could “still try to present to the public that they have an arm’s length relationship with this company, this vendor.”

Self-delusion merging into corruption is one issue, but Gordon thinks the larger picture is more alarming. “The problem is that the vendors [have] had an influence over just about every aspect of the nation’s voting systems, [including the] security of those systems,” he said. “The way in which testing is done on their equipment [is] not the way that a white-glove testing agency would handle certification of their equipment.

“I think that what happens here,” Gordon continued, “is that [as] the relationships develop, there is a breakdown in the arm’s length relationship, and they almost end up on the same team.”

Gordon, who retired from the McClatchy newspaper chain after two decades of investigative reporting, says he doesn’t want to single out any specific individual, instead describing “the general process by which industries have their way with government.” According to Gordon, “it’s disturbing, and it’s especially disturbing at a time when the public is losing confidence in the government’s ability to ensure that they get their most sacred right as citizens: to vote.”

### ***How do lobbying relationships affect voting machine procurement (and voters)?***

Like the Democracy Fund’s Tammy Patrick, Gordon singles out time and budget constraints as important factors that have to be taken into consideration by the people who actually administer elections.

Companies who know the specific details of their own business, as well as the technological issues, clearly have the upper hand when it comes to negotiating with harried administrators.

“They have it all over these people,” Gordon said. “I don’t see how they can be on a level playing field.” In some cases, [administrators] don’t have time to spend on reinventing the wheel. Gordon says that in those situations, election officials want a “turnkey” solution — something that is instantly ready to perform.

If not easy prey, county and state officials are at least targets who may not be aware of how they “can be manipulated by vendors,” Gordon said. For their part, vendors are driven almost exclusively by sales and profits. Their systems are vulnerable to tampering, but maintaining election security is not on their agenda.

If ideal conditions prevail and the right laws and regulations are combined with vigilant officials in top government positions, the right questions may be asked when a new system is purchased. Unfortunately, those are big ifs. “Once that relationship is forged,” Gordon said, “once ES&S or Dominion or Hart InterCivic gets a contract with somebody, it’s hard to break it.”

## Notes

1. [“Lululemon Customers Asked ‘Who Is John Galt?’”](#) *All Things Considered*, NPR, November 17, 2011.
2. Jessica Huseman, [“The Market for Voting Machines Is Broken. This Company Has Thrived in It.”](#) *ProPublica*, October 28, 2019.
3. [“Questions?”](#) News Media Resources, Election Systems & Software, accessed July 2020.
4. [“Re: Ownership of Election Systems & Software, LLC \(‘ES&S’\)”](#) Florida Fair Elections Coalition, June 21, 2019.
5. [“About,”](#) McCarthy Capital, accessed April 20, 2020.
6. Kim Zetter, [“Diebold Unloads Beleaguered Voting Machine Division,”](#) *Wired*, September 3, 2009.
7. [“Justice Department Requires Key Divestiture in Election Systems & Software/Premier Election Solutions Merger,”](#) US Department of Justice,

March 8, 2010.

8. ["Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets From ES&S,"](#) *BusinessWire*, May 20, 2010.
9. ["Company,"](#) Dominion Voting, accessed April 21, 2020.
10. ["In the Field,"](#) Dominion Voting, accessed July 2020.
11. ["Dominion Voting Systems, Inc.,"](#) Business Directory, Dun & Bradstreet, accessed April 21, 2020.
12. Brad Friedman, ["On Heels of Diebold/Premier Purchase, Canadian Firm Also Acquires Sequoia, Lies About Chavez-Ties in Announcement,"](#) *Truthout*, June 21, 2010.
13. ["The Trouble with Touch Screens \[Transcript\],"](#) *Dan Rather Reports*, August 14, 2007.
14. Kim Zetter, ["Sequoia Voting Systems Responsible for 2000 Presidential Debacle?"](#) *Wired*, August 15, 2007.
15. Gabriella Novello, ["Georgians Demand Secretary of State Re-Examine Voting System,"](#) *WhoWhatWhy*, August 20, 2019.
16. ["Hart InterCivic Inc.,"](#) *Bloomberg*, accessed April 21, 2020.
17. ["Press Releases,"](#) Hart InterCivic, accessed July 2020.
18. ["About Us,"](#) H.I.G. Capital, accessed April 21, 2020.
19. Taylor Hatmaker, ["Texas has a long history of problems with Hart eSlate voting machines,"](#) *TechCrunch*, October 27, 2018.
20. ["Trips To Vegas And Chocolate-Covered Pretzels: Election Vendors Come Under Scrutiny,"](#) *Morning Edition*, NPR, May 2, 2019.
21. ["Frequently Asked Questions \(FAQ\),"](#) Voatz, accessed April 22, 2020.
22. Michael Specter, James Koppel, and Daniel Weitzner, ["FAQ on the Security Analysis of Voatz,"](#) Internet Policy Research Initiative, Massachusetts Institute of Technology, February 14, 2020.
23. Morgan Enos, ["Shadow Inc.: How a company with 120 Facebook likes ended up at the center of the Iowa caucus firestorm,"](#) *Fortune*, February 6, 2020.
24. ["Our History,"](#) Smartmatic, accessed April 22, 2020.
25. Kevin Monahan and Cynthia McFadden, ["Has Los Angeles County just reinvented voting?"](#) NBC News, May 2, 2019.
26. Kim Zetter, ["Los Angeles County's risky voting experiment,"](#) *Politico*, March 3, 2020.
27. Drew DeSilver, ["U.S. trails most developed countries in voter turnout,"](#) Pew Research Center, May 21, 2018.
28. R. Doug Lewis, ["Local Officials Must Remain in Control of Elections,"](#)

*New York Times*, November 2, 2012.

29. [Help America Vote Act of 2002](#), Election Assistance Commission.
30. ["The Business of Voting,"](#) Penn Wharton Public Policy Initiative, March 15, 2017.
31. Ibid.
32. ["The Process of Procuring and Implementing Voting Systems,"](#) Election Assistance Commission, November 2019.
33. ["Procuring and Implementing Voting Systems,"](#) Election Assistance Commission, November 2019.
34. ["Electronic Poll Books | e-Poll Books,"](#) National Conference of State Legislatures, October 25, 2019.
35. Jonathan Lai, ["Philly voting-machine vendor lobbied for years to win contract, city watchdog's investigation finds,"](#) *Philadelphia Inquirer*, September 25, 2019.
36. ["Voting Technology Procurement Investigation,"](#) Office of Philadelphia Controller Rebecca Rhynhart, September 25, 2019.
37. Ibid.
38. Marc Levy, ["Judge hears arguments over Philadelphia's voting machines,"](#) Associated Press, February 18, 2020.
39. Jonathan Lai, ["Philly voting-machine vendor lobbied for years to win contract, city watchdog's investigation finds,"](#) *Philadelphia Inquirer*, September 25, 2019.
40. Jennifer Cohn, ["New 'Hybrid' Voting System Can Change Paper Ballot After It's Been Cast,"](#) *WhoWhatWhy*, March 19, 2019.
41. "Greg Gordon, Amy Renee Leiker, Jamie Self, and Stanley Dunlap, ["Voting machine vendor treated election officials to trips to Vegas, elsewhere,"](#) McClatchy Washington Bureau, June 21, 2018.
42. Jonathan Landay and Mark Hosenball, ["Russia, China, Iran sought to influence U.S. 2018 elections: U.S. spy chief,"](#) Reuters, December 21, 2018.
43. [Disposition, COIB Case No. 2018-904](#), New York City Conflicts of Interest Board, accessed July 2020.

2.

## THE VOTING MACHINES

---

### *How do voting machines really work?*

So now we're going to get into the nitty-gritty. A warning to the faint of heart: It's going to get technical as we explore the mechanics of the machines themselves.

Most states are moving toward mail-in voting and toward paper ballots which are read by **optical scanners** after being hand-marked at the polling station. But there are two types of **electronic voting machines** that we will focus on here: the **direct-recording electronic** (DRE) machine and the **ballot-marking device** (BMD).

The DRE machines are the more controversial option. They work in one of three ways: Voters can press a button, register their vote on a touchscreen, or use a dial. Most voters are given the touchscreen option. Votes are then stored on the computer memory of the machines themselves, which are later reviewed by poll workers when gathering the final vote count.<sup>1</sup>

Some DRE machines can be configured to produce a Voter-Verified Paper Audit Trail (VVPAT) in addition to recording votes on a computer memory. These machines let voters mark their ballots on a touchscreen, and then print their ballots for review before putting them through an optical scanner for tabulation.<sup>2</sup>

BMDs, on the other hand, automatically produce a physical ballot with selections made on an electronic or touchscreen surface. As



with a DRE, voters interact with a touchscreen surface to mark their choices.

VotingWorks, a nongovernmental organization developing open-source voting technology, is currently working on a novel software design for tablets — such as an Apple iPad or Google Chromebook — so they can operate like the voting machines we use today.<sup>3</sup> The company already offers software coding for BMDs and vote-by-mail systems.

Another company, Smartmatic, offers a BMD called the Premium Voting Machine.<sup>4</sup> These machines can be configured to skip the paper trail and function like a DRE. They have a barcode reader option for printed ballots. The machines are equipped with a 17-inch touchscreen and smart card, also known as a magnetic memory card — but more on that later.

Some election commissions have developed their own version of the BMD. In Los Angeles County, CA, officials spent more than \$280 million<sup>5</sup> to create the Voting Solutions for All People (VSAP) system, which the county proudly boasts provides voters with “the option for where, when, and how to vote.” They are not connected to the internet, and they allow voters to adjust the size and font on the device’s touchscreen. The machines also are capable of showing candidates from up to six parties in 13 languages.<sup>6</sup>

In addition, the system lets a voter download a sample ballot and fill it out in advance. This can be done on a voter’s smartphone or computer. Voters then receive a “poll pass” and can simply scan the barcode attached in order to verify that their choices are accurate.<sup>7</sup> The advantage is that voters don’t need to wait in line or touch voting machines — thus this technology addresses a concern that election officials throughout the country raised as the coronavirus spread throughout the United States.



ES&S ExpressVote ballot-marking device. Photo credit: Douglas W. Jones / Wikimedia

### ***What is the real difference between a DRE and a BMD?***

While the main difference between a DRE machine and a BMD is how the record is stored, BMDs automatically produce a paper trail by default. However, DREs have evolved and some “can be equipped with Voter-Verified Paper Audit Trail (VVPAT) printers that allow the voter to confirm their selections on an independent paper record before recording their votes into computer memory,” according to Verified Voting. “This paper record is preserved and, depending on State election codes, made available in the event of an audit or recount.”<sup>8</sup>

Georgia computer scientist Richard DeMillo, a leading election security expert, notes that there really is no difference from a technical point of view. Both machines operate along similar lines, although vendors are reluctant to admit that. It is especially difficult to learn more about BMDs, because research has largely been based on taking out-of-use DREs and reconfiguring them to function as BMDs.

For example, when Dominion was bidding for the contract to provide Georgia with equipment for the 2020 election, its marketing materials claimed it was possible to reconfigure Dominion's BMDs so that they also do not leave a paper trail, effectively converting them to act like DREs. (Sales materials from Dominion and competing companies that did not win the contract were posted on a website maintained by Georgia's secretary of state.)

One document submitted by Dominion stated that the company's BMDs "have secure access to internal memory and removable memory components," and require a two-factor authentication to access the "removable memory."

"From the point of view of a computer scientist, there really isn't much difference," DeMillo told *WhoWhatWhy*.

In Philadelphia, for example, officials rolled out new voting machines in November 2019 (an off-year election) that are defined as BMDs, but what is displayed on their screens essentially looks like a keno board. Dr. Rebecca Mercuri, an election security expert for more than 40 years and founder of Notable Software, described the voting experience as feeling "like you're betting on numbers 1, 47, or whatever."

"It's this grid, very hard to read, and ... there were long lines at the polls," Mercuri told *WhoWhatWhy*. The distinguishing feature of the

machines, Mercuri observed, is that “instead of printing out a paper ballot, there is supposedly a paper ballot printed inside the machine and the voter really never gets to see [it].”

### ***How old is most of the election equipment used in the United States?***

According to a report by New York University’s Brennan Center for Justice, published in March 2019, voting machines in at least 40 states are at least a decade old.<sup>9</sup>

Like the voting machines themselves, much of the software used in election equipment has a relatively short lifespan. Vendors usually provide updates every few years, but much of this information is proprietary and, therefore, little information is available publicly.

### ***What is a magnetic memory card?***

Think of the magnetic key cards that open a hotel room. Instead of inserting the card into a hotel room door, you insert the card into a slot in a voting machine and a ballot with the choices you are authorized to vote on appears on the screen.

When voters enter a polling place, they use a stylus to sign in to an electronic poll book (e-poll book). The poll workers then generate a magnetic memory card, which is inserted into the voting machine to register the vote.

The voter’s precinct and ballot appear on the voting machine’s screen when the card is inserted, but the card retains no personal information about the voter.

### ***What are the characteristics of the software used in touchscreen voting machines?***

Not only is voting machine software beyond the capacity of the average voter to understand, most poll workers don't understand it either.

Voting machine software is a tightly held industry secret. We know that DREs run on serial computer processing — meaning only one thing can happen at a time — so things become a little tricky when long lines form at a polling place and the only voting method available is one of these machines. The machines cannot multitask or handle multiple inputs of information, so everyone must wait until the previous voter has completed each step before they get a turn.

### ***Who manufactures the components that go into a voting machine?***

While most of the parts and the software that go into voting machines are still assembled in the United States, many vendors increasingly rely on a global supply chain because “Made in the USA” has become prohibitively expensive.<sup>10</sup>

The Big Three manufacturers are extremely reluctant to release details about their manufacturing processes.

But a market report by the supply chain risk management company Interos, published in December 2019, concludes that up to 20 percent of the equipment that goes into voting machines is made in China.<sup>11</sup> That includes control boards, voting machine software,

and touchscreens. The same report found that roughly 14 percent of suppliers are based in Russia.

In 2019, ES&S publicly acknowledged that their equipment is partially manufactured overseas. Kathy Rogers, ES&S's senior vice president of government relations, insisted in a letter to NBC News in October 2019 that "all tabulation software is developed and compiled exclusively in the USA," and "all final hardware configuration and assembly is performed exclusively in the USA."<sup>12</sup>

In the same letter, however, Rogers acknowledged that ES&S does have a global supply chain, and at least one of its manufacturing sites is based in China. In fact, "some components (such as surface mount capacitors, resistors, inductors and fixed logic devices) may be sourced from China-based manufacturers."

Rogers neglected to mention that some parts are also manufactured in the Philippines — a detail that emerged from NBC's analysis of the company's shipping records.<sup>13</sup>

According to ES&S, the company takes pride in ensuring its equipment meets state and federal standards. Rogers's letter to NBC claimed that the hardware components for election equipment receive verification that there are no alterations and pass the company's "end-to-end [quality assurance] test." The US Election Assistance Commission (EAC) also performed an "onsite audit" of ES&S's overseas manufacturing site.<sup>14</sup>

### ***What is an election management system?***

Election management systems (EMS) offer a one-stop shop for officials who need to supervise ballot designs, voter registration

lists, and a number of other administrative tasks needed to carry out an election. The purpose is to manage all aspects of election administration in one place. The Big Three promote the concept as a secure and easy-to-use option.

ES&S provides the following description of its election management system, Electionware, on its website:

Electionware enables election officials to create a secure election information database, format ballots, program voting and ballot-scanning equipment, consolidate tabulator results, generate election night reports and review ballot images.<sup>15</sup>

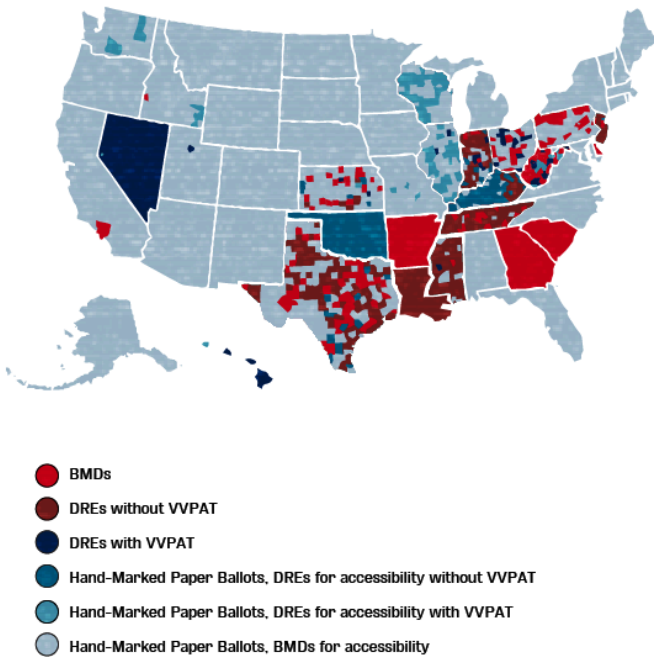
ES&S also promotes Electionware as having “the very latest in election security, including heightened audit controls and built-in change management processes that ensure election data is safe and secure.”<sup>16</sup>

Dominion Voting Systems offers a management system known as Democracy Suite. According to the company’s description there are two key features: an “Election Event Designer” application and a “Result, Tally and Reporting” application.

Democracy Suite has internet connectivity built into its system, which enables election officials to relay information to polling places across their states. Per Dominion’s website, its EMS is “used to design and set up an election, as well as tally and report the results of the election for any of Dominion’s voting platforms.”<sup>17</sup>

These systems are incredibly complex and require extensive testing to ensure there are no cybersecurity concerns.

## WHICH KIND OF MACHINES DO VOTERS USE TO VOTE?



Source: <https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020>

### *How do most Americans cast a ballot?*

After the controversy surrounding the 2016 presidential election, the trend moved from the direct-recording electronic machines toward the ballot-marking devices. Concerns about possible



Russian meddling raised concerns that foreign governments might try to hack American elections by *literally* hacking into voting systems.

In many states, voters still appear at polling places in person to cast their ballots. Usually, voters whose precincts use touchscreen machines head to their designated polling place, receive their magnetic memory cards, and wait for their turn to begin the process. This year that scenario could be different given the COVID-19 pandemic.

If more states eliminate the obstacles that previously made absentee voting next to impossible for hundreds of thousands of voters, we could see fewer people at the polls and more people voting by mail this November.

For the moment, however, the United States finds itself relying on a hybrid approach. The Trump administration has argued forcefully against absentee ballots, also known as vote-by-mail, even though Trump used an absentee ballot himself when he voted in the 2020 Florida primary election, and he has requested an absentee ballot for the general election as well. Vice President Mike Pence also voted by mail in this year's primaries. It is highly likely that the 2020 election will see a mix of absentee ballots and in-person voting using either hand-marked paper ballots or touchscreen voting machines.

In recent years, most DRE machines have been phased out, and about 70 percent of all election districts in the US use hand-marked paper ballots that are supplemented by an accessible device, like a BMD.<sup>18</sup>

### ***Why is there a QR code on my ballot?***

If you've cast a vote via a BMD, you probably noticed something that resembles a barcode on your ballot. That barcode holds your vote choices, and poll workers rely on that to count the vote totals.

There is a considerable debate over whether the QR code is really suitable for tabulating votes. Voting-machine vendors — not surprisingly — insist that the QR code is a fast, easy way to get the job done. Richard DeMillo suggests that the QR code can be compared to a computer printout used as a ballot — as opposed to a paper ballot on which a voter directly makes marks.

QR codes can also be used to prepare ballots before a voter even has a chance to get close to the BMD. In Los Angeles, for example, a voter can scan a QR code on their mobile device that is used to produce a poll pass, which contains a voter's designated ballot. If desired, a voter can even pre-fill the ballot and then verify the choices on it when the poll pass is scanned on the BMD.

### ***What are electronic poll books?***

Electronic poll books, also known as e-poll books, are tablet-like devices, similar to an iPad. E-poll books vary depending on the jurisdiction but, for the most part, they are used for three reasons: signing in a voter electronically, confirming a voter's registration and designated polling place, and double-checking whether a voter has already submitted an absentee ballot that has been accepted.

E-poll books are fairly easy to use. They are about the size of a standard tablet, and allow poll workers to quickly confirm or update voter information within minutes.

According to the National Conference of State Legislatures, some e-poll books are also networked and can receive immediate updates on who has voted in other voting centers.<sup>19</sup> The bottom line is that some states employ e-poll books that can be operated remotely and have internet connectivity. The risk is that connecting voting devices to the internet significantly increases the system's vulnerability to hacking.

### ***What role do optical scanners serve in the voting process?***

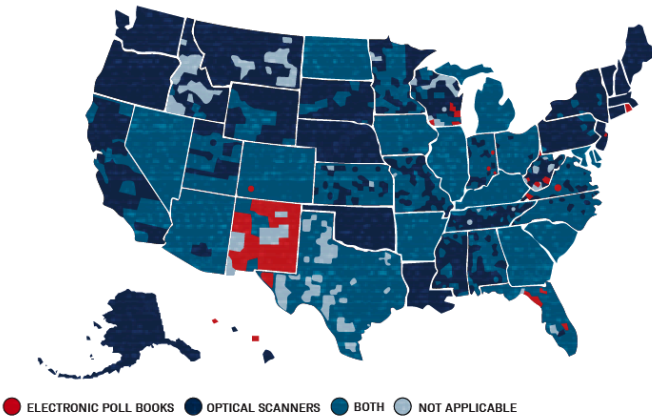
Optical scanners are machines that make digital images of ballots so they can be counted. They look very much like a typical photocopy machine, and they are usually used to tabulate ballots produced by BMDs.

Voters either mark their choices by hand on paper ballots, or they use a BMD to do the marking for them. The completed ballots are then run through the scanner, which takes a digital image and tabulates the votes in real time. Sometimes the scanning takes place right at the precinct, sometimes at a centralized location for the county, like the board of elections office.

At the end of the day, when all of the ballots are counted, poll workers print out a receipt with the totals. The total number of votes is then compared to the number of voters who were checked in throughout the day; the same as is done with DREs. If those numbers match, then election officials begin certifying the results.

In contrast to the optical scanners that resemble copy machines, some optical scanners are built directly into DREs in order to tabulate and store votes in real time.

## WHICH STATES ARE USING E-POLL BOOKS, OPTICAL SCANNERS, OR BOTH?



Source: <https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx>  
 Source: <https://verifiedvoting.org/verifier/#mode/search/year/2020>

### *Which states use e-poll books and optical scanners?*

In most elections, poll workers are primarily concerned with moving the maximum number of voters through the process as quickly and efficiently as possible. Because they theoretically speed up the voting process, e-poll books and optical scanners are extremely popular and are now in widespread use. The process begins with the e-poll books.

During the 2016 presidential election, seven states and two territories (Colorado, Georgia, Maryland, Michigan, Nevada, South Carolina, Rhode Island, the District of Columbia, and the US Virgin Islands) used e-poll books in all their election districts. Another 36

states used e-poll books in at least one jurisdiction. To date, Maine is the only state that does not allow the use of e-poll books anywhere in the state — due to cybersecurity concerns. Additionally, eight states (Alaska, Hawaii, Louisiana, Montana, Oklahoma, Oregon, Vermont, and Washington) do not explicitly prohibit the use of e-poll books but generally do not use them.<sup>20</sup>

According to the EAC's latest annual report, issued in July 2019, e-poll books are now being used in a growing number of election districts. More than a quarter of election jurisdictions reported using e-poll books during the 2018 midterm elections. In fact, the use of e-poll books shot up by nearly 50 percent between the 2014 and 2018 elections.

The Big Three make slightly different versions of e-poll books and optical scanners. Smaller companies vary in whether they sell either, and a few jurisdictions have developed their own versions. Meanwhile, nearly every state relies on an optical scanner as part of their voting system. New Mexico is the only state to date in which only a few jurisdictions use them.

### ***What states still use DREs or BMDs?***

Fourteen states used completely paperless voting machines during the 2018 midterms.<sup>21</sup> Others have or are currently considering whether to replace the machines with hand-marked paper ballots. Voting-rights groups have filed several lawsuits to expedite the process because they claim that the voting systems in use are not foolproof.

In Georgia, for example, we saw what happened when 30,000 new touchscreen voting machines were used during the state's recent

presidential primary election. Technical problems caused machines to malfunction or break down altogether.<sup>22</sup> Also, the voting machines produce a QR code, which (instead of the human-readable portion printed on ballots) represents the final vote, so it is effectively impossible to audit the system. Even when paper is involved in the voting process, as it was with absentee voting in Georgia, the ballot scanners misread hundreds of ballots or incorrectly flagged ballots because of programming issues.<sup>23</sup>

The elections group Verified Voting has an interactive database, known as the Verifier, on its website so voters in any jurisdiction can learn more about the election equipment they'll be using to cast their vote.<sup>24</sup> The data suggests that the country overall is moving toward a paper-based voting system, and optical scanners continue to be a popular tool for tabulating votes.

For example, voters in Arkansas, Georgia, and South Carolina will use BMDs this November. That's not to say every state has abandoned the use of paperless voting machines. Louisiana, Mississippi, Tennessee, and New Jersey are just some of the states that will still offer DREs in at least one county.

### ***How are votes stored on paperless voting machines? How are they counted?***

Thankfully, it's a fairly straightforward process. DRE machines tabulate votes inside the machine itself in real time. After the last voter has cast his or her ballot and the polls close, the tallying begins. Poll workers go to each machine to check the screens for the number of votes cast and compare those totals with the number of ballots that went through the optical scanners.

In an ideal world, it is just that simple. “The vote is then either stored on a magnetic card or sent via USB cable to a printer,” DeMillo said.

Unlike DREs, ballot-marking devices (BMD) do not store votes in real time on the voting machine. Instead, when the voter fills out the ballot on the BMD, the machine prints a receipt with the QR code plus readable text listing the voter’s choices in plain language. What constitutes the actual vote, however, varies by state. In Georgia, for example, election results are based on what the QR codes contain — and it is impossible to know whether the QR code contains the same information as what the readable text says.<sup>25</sup>

## Notes

1. [“Voting Machine Technology,”](#) American Association for the Advancement of Science, accessed April 2020.
2. [“Voting Equipment in the United States,”](#) Verified Voting.
3. Jason Koebler, [“This MIT PhD Wants to Replace America’s Broken Voting Machines with Open Source Software, Chromebooks, and iPads,”](#) *VICE News*, November 6, 2018.
4. [“Smartmatic Premium Voting Machine — Product Overview,”](#) Smartmatic, accessed April 2020.
5. Neena Satija and Joseph Marks, [“Los Angeles County’s new voting machines hailed for accessibility, dogged by security concerns,”](#) *Washington Post*, March 3, 2020.
6. [“Voting Solutions for All People,”](#) County of Los Angeles, accessed April 2020.
7. Ibid.
8. [“Voting Equipment in the United States,”](#) Verified Voting, accessed April 2020.
9. Lawrence Norden and Andrea Cordova McCadney, [“Voting Machines at Risk: Where We Stand Today,”](#) NYU Brennan Center for Justice, March 5, 2019.
10. [“The facts about supply chain and manufacturing of voting systems,”](#) Election Systems & Software, accessed April 2020.

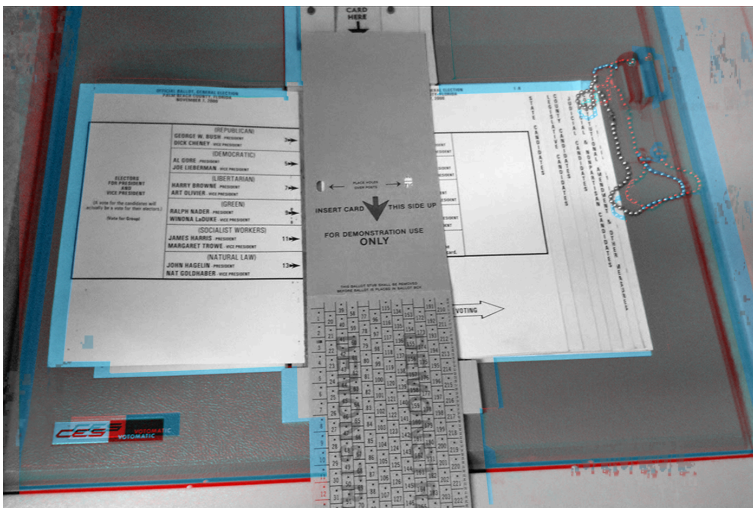
11. Harris Allgeier, "[Interos study finds that 20% of voting machine components come from China-based companies](#)," Interos, December 16, 2019.
12. "[ES&S Letter to NBC](#)," October 15, 2019.
13. Ben Popken, Cynthia McFadden, and Kevin Monahan, "[Chinese parts, hidden ownership, growing scrutiny: Inside America's biggest maker of voting machines](#)," NBC News, December 19, 2019.
14. "[The facts about supply chain and manufacturing of voting systems](#)," Election Systems & Software, accessed April 2020.
15. "[Electionware](#)," Election Systems & Software, accessed April 2020.
16. "[Electionware Security Bulletin](#)," Election Systems & Software, accessed April 2020.
17. "[Democracy Suite](#)," Dominion Voting Systems, accessed April 2020.
18. "[The Verifier](#)," Verified Voting, accessed April 2020.
19. "[Electronic Poll Books | e-Poll Books](#)," National Conference of State Legislatures, October 25, 2019.
20. Ibid.
21. Eric Geller, Beatrice Jin, Jordyn Hermani, and Michael B. Farrell, "[The Scramble to Secure America's Voting Machines](#)," *Politico*, August 6, 2019.
22. Darlena Cunha, "[Activists Worry New Georgia Voting Machines Open To Cyberattack](#)," *WhoWhatWhy*, June 29, 2020.
23. Gabriella Novello, "[Georgia Certifies Election Results Despite Serious Flaw in Ballot Scanners](#)," *WhoWhatWhy*, June 23, 2020.
24. "[The Verifier](#)," Verified Voting.
25. Mark Niese, "[Georgia election officials approve computer recounts of paper ballots](#)," *Atlanta Journal-Constitution*, March 1, 2020.



3.

## VOTING MACHINE ACCESSIBILITY

---



Punch card for Palm Beach County Votomatic machine used in 2000 Presidential election. Photo credit: [Clariosophic / Wikimedia \(CC BY-SA 3.0\)](#)

### *Why have different types of voting machines?*

Simply put, not everyone can vote the same way.

Not every voter speaks and reads English, so voting machines need to be able to show ballots in a variety of languages. Some voters

need hearing assistance or buttons on a machine to mark their choices if a touchscreen or pencil is not an option.

To meet the needs of voters, there are two federal statutes — the Help America Vote Act (HAVA) and the **Americans with Disabilities Act** (ADA). This chapter focuses on HAVA.

### ***How did the Help America Vote Act change voting in the United States?***

In 2002, President George W. Bush signed the Help America Vote Act, and the US Election Assistance Commission (EAC) came to life. The law was intended to prevent controversies, such as those that surrounded the 2000 election, from happening again.

HAVA changed how ballots are cast. The law requires voting systems to keep their error rate extremely low.

HAVA revamped the standards for testing and certification, and it transferred responsibility for setting the standards for quality assurance to the EAC.

HAVA also ordered that lever and punch-card machines should be phased out. Votomatic's punch-card voting system was specifically listed as one of the machines to be eliminated. As it turned out, Votomatic's vote system was absorbed by ES&S along with a number of other companies. According to Verified Voting, the banned system — now under a different name — was used during the 2014 midterm elections.<sup>1</sup>

One of the controversies surrounding the punch-card machines was that the system's tendency to overreport or underreport votes often occurred in communities of color, because the voting systems there

were in worse condition than in counties that could afford more advanced options. The EAC set an error rate for voting systems — between one in every 10 million ballots and one in every 500,000 ballots — in its federal voting systems guidelines.<sup>2</sup>

Once the error rate was introduced, “lever machines and punch-card machines were phased out because people who manufactured them weren’t going to have them tested,” Marian K. Schneider, president of the governance group Verified Voting, said.

### ***What are the Voluntary Voting System Guidelines?***

Why is it possible to do banking on your mobile device but impossible to vote on a smartphone? The answer has something to do with HAVA, which obligated the US Election Assistance Commission to establish and maintain federal guidelines for election equipment. The guidelines, known as the **Voluntary Voting System Guidelines** (VVSG), set the specifications for testing voting systems to ensure that they provide basic functionality, accessibility, and security protections.<sup>3</sup>

The guidelines might have provided a level playing field for voting across the entire country, except that they are not mandatory. There is no penalty if a state decides not to comply.

Because the federal government moves slowly, and standards vary in the states that do have their own certification processes, the time it takes for voting system guidelines to be updated can take months. In some states, like California, it can take more than a year for officials to certify voting systems.

"It depends whether the system has already had federal certification," Schneider said, "but it's measured in months. It's not days, it's not weeks."

Voting-machine vendors who focus on the national market tend to pay more attention to the federal certification process. Since many states cannot afford the cost of independent testing, many election officials count on federal certification as proof that the voting systems work. For example, the Pennsylvania Department of State will not approve a new voting system in the state unless it has been certified by the EAC and Pennsylvania secretary of state.<sup>4</sup> That said, there are states that rely primarily on their own certification processes, and, in a handful of states, no certification process is required at all.<sup>5</sup> The guidelines are little more than a patchwork of recommendations.

The certification process itself is far from uniform. When it comes to the testing required for federal certification, the EAC has been trying to revise the process for some time.

Federal standards are reviewed every few years. In September 2016, the EAC's Technical Guidelines Development Committee (TGDC) approved a proposal to draft new guidelines. In March 2020, EAC commissioners held a virtual meeting to discuss what is being called VVSG version 2.0.

### ***How far ahead of an election is the equipment actually installed in the polling place? Where is it stored before the election?***

In an ideal setting, election equipment is sent to polling places at least one week prior to an election so officials can set up voting

machines, program e-poll books, and make certain that all poll workers are trained to help voters who need assistance. It doesn't always happen that way. In Georgia's June primary election some polling places only received voting machines on the morning of the election.<sup>6</sup> A spokesperson for Republican Secretary of State Brad Raffensperger's office told *WhoWhatWhy* in February that most of the equipment was on its way, if not already at county election offices — but local news reports contended otherwise.<sup>7</sup> In June, on the day of the primary, local county election boards also told *WhoWhatWhy* that it was common practice for the machines to arrive the day of an election. Unsurprisingly, the hasty setup created problems when voting machines failed to function properly.

In other polling places, where voting machines had been delivered well in advance of the election, the machines have been simply dumped at the polling site and left as easy targets for anyone interested in tampering with the machines.<sup>8</sup> Georgia voting expert Richard DeMillo observed that security in Georgia tends to be a pretty loose affair.

"The secretary of state's office and the county election offices have not been very good at physically locking down the equipment," DeMillo said. He noted that old DREs have often simply been piled up in school gymnasiums where anyone can access the machines.

One of the running themes of the Trump administration has been the fear of widespread voter fraud. There are serious vulnerabilities in US election systems, but the real concern is malicious actors accessing voting technology to cause system-wide problems<sup>9</sup> — not individuals trying to vote twice or noncitizens getting access to ballots.<sup>10</sup> In other words, the concern is *election* fraud, not *voter* fraud. And the way voting machines and election equipment are

stored in the days leading up to an election puts them at risk of being physically tampered with.

### ***How difficult is it to set up voting machines in a polling place?***

How easy it is to move a voting machine depends on the device. They're all different.

Some BMDs are slightly bigger than an average laptop. Optical scanners tend to be much larger. They may not weigh much, but they can be quite bulky. ES&S's ExpressVote XL, for example, has a 32-inch screen that is placed on a metal cart with heavy-duty wheels.

"The vendors cart them around to trade shows and [meetings with election officials] all over the country, so it can't be that difficult," Schneider told *WhoWhatWhy*. "But some of them are big enough that they have to be delivered well in advance ... there's no way to generalize it."

### ***What quality assurance checks are performed on voting machines before and after an election?***

Most states rely on the federal certification required by the EAC. Some states also require a state-level certification process, but that can be costly and therefore is often outsourced to a third party — like the voting-machine vendors themselves.

To guarantee voter confidence in the system, election officials also need a means of credibly auditing and verifying the final outcome.

A widespread, popular approach is the **risk-limiting audit** (RLA). This is a statistical review of a sample of ballots in order to verify an outcome.

Dr. Philip Stark, a professor of statistics at the University of California at Berkeley and the creator of the RLA, described the process to *WhoWhatWhy* as using a random sampling of paper ballots to double-check the results reported by the voting machine. If the sampling of paper ballots statistically confirms the machine's results, you can be pretty certain that you have identified the winner.

"Let's just assume it's a plurality contest," Stark said. "Alice is running against Bob and Alice is purported to have won. How can we check whether that's true for this pile of paper? The machines reported that Alice won. Does the paper support that? So, if we started to pull ballots at random from the pile, and we pulled a ballot ... for Alice 20 times, that would be incredibly unlikely to happen if Bob had actually won. So, that's strong evidence that if you tabulated all of the votes accurately, it would show that Alice won."

In other words, officials check to see if there is convincing evidence that there is a majority of votes for one candidate or the other.

"In order for it to be very unlikely to see that many for Alice if Bob had actually won, that's where the math is," Stark explained. "So ... what makes it a risk-limiting audit, is the stopping rule that says, 'OK, I've seen enough,' is set up in such a way that the probability that it stops without a full hand count is small, say five percent, if Alice didn't really win. That kind of rule is the risk-limit."

A growing number of states have begun implementing RLAs. Rhode Island passed legislation requiring that RLA guidelines be applied to all audits during the 2020 election. That was after the previous

approach resulted in an embarrassing failure during a 2016 referendum.

The referendum resulted in 8,471 “no” votes and only five votes in favor of the referendum.<sup>11</sup> The actual count was 9,492 votes in favor and 4,569 “no” votes. The issue was discovered when a working group was established and three RLA pilot tests were run in January 2019.<sup>12</sup>

As it turned out, this was the result of a programming error — election administrators changed the default answers for questions on the ballot from “accept” or “reject” to “yes” or “no,” but the tabulator was reading the wrong ovals on the ballots.

### ***What instructions do voters need to use a voting machine? Are there multiple language options for non-English-speaking voters?***

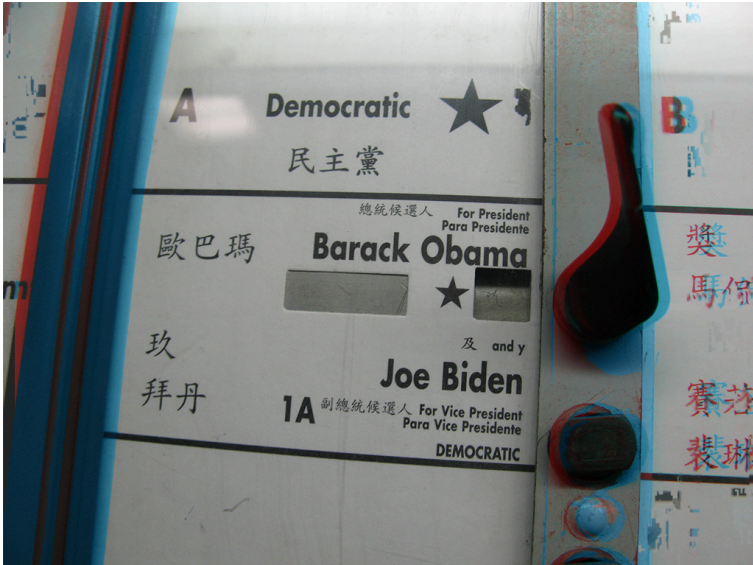
Poll workers are expected to assist voters who need help casting their ballots. Some voters may not speak English well, so instructions on how to vote are usually posted in the voting booth or on the screens of the voting machines themselves. The instructions and the ballots need to be available in different languages, according to the Voting Rights Act of 1965.

States determine which counties need instructions in additional languages, and they decide which languages need to be included on ballots. The decision is usually based on census data.

Verified Voting’s Marian K. Schneider says that she has seen English and Spanish on the same ballot when paper ballots are used. “I believe usability and language experts have said that is the way it



should be — right next to each other because ... translation doesn't always go perfectly," Schneider said.



New York state lever-action voting machine, 2008. Photo credit: [Nick Normal / Flickr \(CC BY-NC-ND 2.0\)](#)

### ***How accessible are voting machines for voters with disabilities?***

Polling places must have accommodations to allow all voters access to the ballot box, regardless of the size of a jurisdiction.

This requirement falls under Title II of the ADA, which “prohibits discrimination on the basis of disability in all services, programs,

and activities provided to the public by State and local governments, except public transportation services.”<sup>13</sup>

In other words, elections must be free and accessible to all voters. Unfortunately, that is not always the case.

In Florida, Notable Software’s Dr. Rebecca Mercuri saw many older voters struggle to use BMDs during a public demonstration without assistance from poll workers.<sup>14</sup> Dexterity issues, for example, can make holding a stylus pen to sign into an e-poll book or pressing buttons difficult for elderly voters or voters with disabilities.<sup>15</sup>

During the 2004 election in California, Mercuri also saw that blind and vision-impaired voters had been required to cast their votes on a BMD by selecting a “yellow button.” Disability rights groups frequently complain that voting systems don’t respond to the physical needs of their voters.

The EAC requires a usability test for voting systems, Schneider says, but vendors are responsible for completing and submitting these tests. “So, it’s not exactly an outside test in my view,” she said.

### ***Can voters still write in a candidate's name on a touchscreen voting machine?***

In the event that a voter is unhappy with any of the choices for candidates listed and wants to cast their ballot for a candidate that is not listed, it is a fairly easy process. All voting machines are required by law to let voters add a write-in candidate’s name to their ballot. The requirement holds whether votes are marked on a paper ballot, recorded on a screen, or delivered by pushing a button.

When voters start marking their choices on an electronic voting machine, the size of the candidates' names can be changed to their preference. If too many candidates are shown on the screen at one time, an arrow or button allows the voter to see the full list of candidates. That is not to say that voters are always aware of this — in 2018, some Kansas voters left their polling places frustrated because they had to touch a button that said “more” to view all of the candidates.<sup>16</sup> But, that was in part due to a software glitch that prevented all of the candidates from fitting on one page.

### ***How well trained are poll workers when it comes to assisting voters?***

Most training is performed perfunctorily either with a brief in-person training session, or simply by asking the poll worker to read an instruction manual. The training, in short, could be much better, especially when it comes to preparing poll workers to assist voters with disabilities.

Schneider, who worked for Pennsylvania's Department of State from 2015 to 2017, recalls that when disability rights organizations met with election officials she was able to distribute a video highlighting the special needs of disabled voters. “The main message,” she said, “was how to respect people with disabilities when they come to vote. I think it's an essential component.”

Disability rights groups nevertheless argue that poll workers are often woefully untrained to assist disabled voters.

Schneider noted: “If a machine is not set up or the poll worker doesn't know how to use it, they have a very poor experience. So, it's absolutely essential that poll workers be trained.”

## ***What does it mean to have the right to a “secret” ballot?***

A ballot, once it is cast, must be completely anonymous if our elections are to be absolutely free and protect voters from outside influence or retaliation. That’s why old-style voting systems had you mark the ballot in a booth behind a closed curtain or required you to seal the ballot from view before depositing it in a box. In fact, a majority of states mandate the right to secrecy when a voter casts their ballot.<sup>17</sup>

Modern voting machines can complicate the question of anonymity. In principle the voting machine needs to record the vote while maintaining the anonymity of the voter. That may be easier said than done, and it has been a hotly debated subject when looking at the machines chosen by different election commissions and how each machine functions.

## Notes

1. [“Votomatic,”](#) Verified Voting, accessed April 2020.
2. [“Voluntary Voting System Guidelines,”](#) Election Assistance Commission, 2005.
3. [“EAC Updates Federal Voting System Guidelines,”](#) Election Assistance Commission, March 31, 2015.
4. [“New Voting Systems,”](#) Votes PA, accessed April 2020.
5. [“System Certification Process,”](#) Election Assistance Commission, accessed April 2020.
6. Nick Corasaniti, [“Georgia Havoc Raises New Doubts on Pricey Voting Machines,”](#) *New York Times*, June 11, 2020.
7. Tia Lynn Ivey, [“Privacy Concerns Plague Voting Efforts,”](#) *Morgan County Citizen*, February 13, 2020.

8. Jordan Wilkie, "[WhoWhatWhy Finds Voting Machines Unguarded](#)," *WhoWhatWhy*, October 15, 2018.
9. [Testimony of Matt Blaze](#), Hearing on Defending Against Election Interference, November 19, 2019.
10. "[The Myth of Voter Fraud](#)," NYU Brennan Center for Justice, accessed April 2020.
11. Gabriella Novello, "[New Report Sets 'Gold Standard' for Election Audits](#)," *WhoWhatWhy*, September 7, 2019.
12. "[Pilot Implementation Study of Risk-Limiting Audit Methods in the State of Rhode Island](#)," Report of the Rhode Island RLA Working Group, August 2019.
13. "[Information and Technical Assistance on the Americans with Disabilities Act](#)," Civil Rights Division, US Department of Justice, accessed April 2020.
14. Gabriella Novello, "[Ignoring Warning Signs: Officials Approve Vulnerable Voting Machines](#)," *WhoWhatWhy*, January 6, 2020.
15. "[Elderly Voters: Some Improvements in Voting Accessibility from 2000 to 2004 Elections, But Gaps in Policy and Implementation Remain](#)," Testimony Before the Special Committee on Aging, United States Senate, January 31, 2008.
16. Dion Lefler, "[Voting Software Makes Some Candidates Harder to Find in Sedgwick County, Kan.](#)," *Government Technology*, August 3, 2018.
17. Caitriona Fitzgerald, Pamela Smith, and Susannah Goodman, "[The Secret Ballot at Risk: Recommendations for Protecting Democracy](#)," Verified Voting Foundation, accessed April 2020.

4.

## VOTING MACHINE VULNERABILITIES

---

### ***How does aging affect a voting machine's ability to function as expected?***

Like any other piece of technology, aging can cause a number of functionality and security concerns. It's like using a computer that was built in the 1990s. It probably would not work at full capacity in 2020, and it is definitely inferior to today's technology.

Election equipment can fail at any time, especially if it has been in use for more than 10 years — and that's without malicious action.

Some equipment failures are caused by incompetence on the part of those who create and handle quality assurance.

Take, for example, what happened at the DEF CON Voting Village's 2018 gathering. This annual event is the largest gathering of white-hat hackers and top cybersecurity experts from around the world. While analyzing the Advanced Voting Solutions (AVS) WINVote system, it took attendees mere minutes to find dozens of machines containing MP3 files that never should have been there, but had existed for years. The AVS touchscreen voting machine was nicknamed "America's worst voting machine" by the gathering's participants.<sup>1</sup>

Thankfully, these machines were taken off the market and are no longer in use as of 2016. But problems like this are not always so easy to identify. As the machines get older, the supply chain becomes narrower, and “you have no idea where the parts are coming from,” Georgia voting expert Richard DeMillo added.

“That’s going to happen to every piece of electronics,” he said.

### ***Why should we be concerned about the chain of custody for election equipment?***

Where were the parts manufactured for the machines we’ve just discussed? As we mentioned earlier, one in five parts needed to maintain our voting machines is manufactured by a company based in China. DeMillo says that researchers examining the machines were able to trace the modules to China because the machines’ memory modules still contained MP3 files in Chinese.

The fact that so many parts used in American voting machines are manufactured in other countries ought to be a cause for some concern, especially as these machines become increasingly computerized. When the original manufacturer discontinues a machine and stops manufacturing replacement parts, the new supply chain could cause risks to election security.

Even if we put the cybersecurity concerns aside, there is yet again the issue of incompetence to worry about.

“There are lots and lots of photographs of unsupervised depositories of these machines,” DeMillo said. “They’ll just be sitting in the hallway of some church or some school.”

A group at Princeton spent many years traveling across New Jersey and New York to take pictures of unattended voting machines, “just to make the point that these are offices that are run by either volunteer labor or people that are not terribly skilled in protecting IT resources,” DeMillo said.

In some cases, old DREs were found unattended in school gymnasiums. Officials claim that they place tamper-indicating seals on the machines to serve as proof that machines have not been infiltrated or altered while in storage, but researchers from the Los Alamos National Laboratory say those can still be “easily spoofed by almost anyone.”<sup>2</sup>

### ***What are some of the pitfalls of the Voluntary Voting System Guidelines?***

Aside from the fact that the standards used for American voting machines were developed more than 15 years ago, one of the biggest pitfalls of the Voluntary Voting System Guidelines is the fact that in the end these guidelines are just that — voluntary. Voting-machine vendors are not obligated to follow them, and often they don’t.

“These are not standards,” said Notable Software’s Rebecca Mercuri. “The [Federal Election Commission] and EAC have never created voting system standards. They are marked guidelines. So, there are no federal standards, and that was deliberate.”

Mercuri added that when the EAC issued its guidelines, the federal government tried to establish standards, but found that it could not even manage to get them accepted for federal elections. Most of the objections centered on “states’ rights.”



With no federal law imposing standards, state and local election officials are constantly tempted to test the EAC's commitment to its guidelines. As Verified Voting's Marian K. Schneider put it, the EAC chose to draft "principles" that it expects voting systems to live up to, but it shied away from prescribing how those principles should be implemented.

The country's inability to agree on national standards has led to spotty quality control.

The North Carolina State Board of Elections certified voting machines from ES&S and Clear Ballot in August 2019. A month later, Clear Ballot withdrew its bid to supply new machines, claiming that the state's certification process was flawed. At the same time, Clear Ballot accused ES&S of being a "virtual monopoly."<sup>3</sup>

ES&S turned out not to have enough machines to fill North Carolina's order, so it offered to replace the certified machines with a different set of machines. ES&S had misled state officials about the company's ability to provide enough of the originally certified machines for the entire state. In January 2020, a spokesperson for the board told *WhoWhatWhy* the company had not behaved improperly, because there was no real technical difference between the certified machines and the machines ES&S provided as replacements.

Not everyone agreed with that. State Rep. Verla Insko (D) told *WhoWhatWhy* that the board had violated the 2005 Confidence in Election law because the new models had not been certified. The allegations were that ES&S had engaged in a tactic that amounted to bait and switch.

"If bait and switch means that we decided to send the most recent and the most secure system to the citizens of North Carolina," ES&S

CEO Tom Burt countered, “then that’s what we did.”<sup>4</sup> Burt may very well have been correct, but since the new machines were delivered without certification, election officials had no way of knowing, one way or the other.

### ***Can extreme weather cause a voting machine to malfunction?***

You bet! During the 2018 election, for example, Florida watched while 3,000 votes disappeared from a single scanning machine simply because it was old and overheated.<sup>5</sup>

That was in Palm Beach County. The vendor accused poll workers of incompetence. But try keeping a laptop or cell phone functioning under extremely high temperatures — if the technology is old, there is a chance that it will overheat and crash. Those vulnerabilities need to be taken into consideration when buying new equipment or deciding to keep using older equipment.

“If you’re storing pieces of electronics in a humid climate above 90 degrees, you’re going to have some amount of voting machines fail,” explained DeMillo, “because they’re not designed to operate in that range. We don’t know what that number is, but it’s a concern.”

One reason we don’t know more about when machines are likely to fail is that the companies that manufacture the machines are reluctant to release proprietary information.

In general, voting machines do not have built-in insulation or self-cooling mechanisms. E-poll books are too small to add a cooling mechanism. As machines age and need to be replaced, some counties are considering replacing them with paper ballots rather

than with newer, even more expensive voting machines. Other counties are not.



Milwaukee County residents line up to vote, April 7, 2020. Photo credit:  
[© Pat A. Robinson/ZUMA Wire](#)

***What are the public health risks from the COVID-19 pandemic when it comes to election equipment?***

Since public health experts continue to raise concerns about the coronavirus, the pandemic's impact on the 2020 election is a natural concern, particularly when it comes to keeping the machines clean and disinfected without compromising their security.

Despite the Trump administration's efforts to downplay social distancing requirements, interest in voting by absentee ballot has

surged across the country. It is reasonable to expect that millions of voters will still be casting their ballots in person this November, although it remains uncertain whether the millions of in-person voters can safely cast a ballot.

Such fears came to life during the primary elections. In Wisconsin, for example, the city of Milwaukee normally operates 180 polling places. In this year's primary elections, that number was reduced to just five, leading to long lines.<sup>6</sup>

State health officials tied dozens of coronavirus cases to in-person voting — and that was just a primary election, in which fewer people typically turn out to cast a ballot.

To try to keep voters safe when touching voting machines, election experts and the EAC have provided guidelines for poll workers, specifying which cleaning products should be used on election equipment.

A number of risks exist despite those guidelines. The coronavirus can remain active on cardboard, plastic, and stainless steel.<sup>7</sup> In recent elections in Georgia, poll workers were forced to shut down the entire system so that Dominion voting machines could be safely cleaned, because that was the best guidance the company could provide to keep the public safe.<sup>8</sup>

"You're voting on the touchscreen that other people voted on before you," Marilyn Marks, executive director of the Georgia-based Coalition for Good Governance, said. "Well, your logical thing would be to say, why don't they clean it between every voter, do a wipe-down?"

That might sound reasonable, but as Marks put it: "You don't really want people touching the same screen as the person before them

touched.” But if every voting machine needs to be restarted after it’s cleaned, then “it’s going to take forever.”

Another concern focuses on magnetic memory cards, which are not disposable. These cards change hands countless times over the course of an election and need to be sanitized between each use.

“You pick up your ballot, now you take your smart card out of the touchscreen, you now go put your paper ballot into the scanner and return your smart card to the poll worker,” Marks explained. “When you do all of that process, you have a lot of touch points.”

### ***How do you hack a voting machine?***

There are quite a few ways in which a malicious hacker or foreign power could disrupt America’s voting process, especially with the newer computerized machines. Voting by mail could reduce the risk of election tampering through cyber hacking, although intelligence officials warn that foreign adversaries are once again “trying to gain access to U.S. state and federal networks.”<sup>9</sup> For the time being, however, there needs to be a serious assessment of the vulnerabilities inherent in the current generation of machines.

Los Angeles’s system, Voting Solutions for All People (VSAP), for example, had dozens of vulnerabilities and security flaws prior to its launch. Investigative reporter David Goldstein, who obtained studies commissioned by the California secretary of state’s office, reported that official testers trying out the system were able to defeat most of the system’s locks and seals almost immediately.<sup>10</sup> Officials had to race against the clock to resolve the problems in time to meet certification requirements for the state’s 2020 presidential primary elections. State officials might have been

alarmed by the system's vulnerabilities, but they were not likely to abandon a system that had cost nearly \$300 million and taken a decade to develop.

Los Angeles County went ahead and used the machines on Super Tuesday. While there were no initial reports of hacking, a number of technical issues led to delays that frustrated voters and poll workers alike.

The findings of the Voting Village at **DEF CON** highlight the need for a serious reexamination of America's voting systems. In 2019, the organizers raised concerns that were graver than ever before. The consensus was that the latest technology for voting systems in the United States had become very vulnerable and its security firewalls were easier than ever to bypass.

One machine that was easily infiltrated at this event was ES&S's Automark ballot-marking device. The lock on this machine is easily picked, and because it is an unencrypted device, there is unrestricted access to the hardware and software.<sup>11</sup>

### ***Why does the shelf life of voting machine software matter?***

The longer a machine is in use, the greater the chance a hacker can discover and exploit its vulnerabilities. In other industries, it is relatively easy to fix vulnerabilities. Businesses update their software every few weeks, and they can always send patches to customers when a new vulnerability is discovered.

This rarely happens in the voting machine industry.

In Georgia, for example, it's fair to say that efforts to patch vulnerable software are inadequate at best. For the moment, there is no publicly available information on whether vendors actively check their equipment for vulnerabilities, or whether the vendors even bother to issue needed software patches. Even a voting expert like DeMillo has a difficult time getting accurate information concerning the maintenance of voting machines.

"When you looked at a software that was running on a machine, you had no idea when it had been patched, whether or not it had been patched in response to a vulnerability," DeMillo said.

"In the commercial world, you know all of that and in some other applications, like defense applications, contractors are really diligent about feeding that information to their customers," he added. "It's not true in election technology and so ... election officials are in the dark as to how current the software is that you're running on your machines."

### ***What are the concerns about magnetic memory cards?***

Just as the ballot design should be the only thing on the smart card before a voter marks his or her ballot, it should also be the only thing on the card once the voter returns it to a poll worker.

If an e-poll book is manipulated, it can be relatively easy to transfer malware to a voting machine through the card.<sup>12</sup> If a voting machine has been tampered with, either physically or remotely, it can transfer malware to an optical scanner and make its way back to the e-poll books.

No one we talked to was able to provide much information about this, because voting-machine vendors usually refuse to let outsiders conduct research on their machines.

Public knowledge of how vulnerable voting machines are to this type of intrusion remains limited, because vendors refuse to let anyone conduct the research. Marks says she is confident that her group will soon have that answer. Since 2018, the Coalition for Good Governance has been fighting Dominion (which sells the magnetic cards) and state election officials, in court, for information disclosure.

### ***What's wrong with counting votes through QR codes on a ballot?***

QR codes make the whole voting process even more opaque. People can't read a QR code on their own — it requires an electronic device capable of deciphering it. If poll workers need to do a recount or to audit the ballots, they rescan the QR codes, not the text below it that lists voters' choices in plain English. It might make more sense to scan the readable text, but that is not the way the machines work.

Election integrity experts have two concerns that focus on the QR code. One is that a QR code is not transparent. DeMillo explains that because the code reporting the actual vote can't be read by the person casting the vote, there is less public confidence in the reliability of the election itself. "That in itself is kind of a bad thing," he said.

The second major concern is that the QR code constitutes an opportunity for mischief. A hacker who wanted to induce chaos in an election could simply introduce software that invalidates the QR



code or makes the QR code report a choice that is different from the printed text on the ballot.

A skilled hacker could conceivably modify the printed text and QR code on ballots at the same time so “you would have no idea what that ballot was going to represent,” DeMillo said.

Even if a DRE is configured to operate as a BMD and provides some form of a verified paper audit trail (VVPAT), storing and counting the votes are left to the discretion of the election officials. This is where the problem gets more complicated.

Los Angeles’s VSAP system is a case in point. The voter goes online to fill out a digital ballot and create a “poll pass,” which can be printed or downloaded. If they choose to download their ballot, they can then upload their pre-filled ballot to the voting machine’s screen for final review by scanning the QR code on that ballot from their phone. “That’s tantamount to allowing vote selling, because anybody can do that and say, ‘Here, use this QR code,’” Mercuri said.

### ***How can voting machine software be manipulated?***

Mounting an attack on voting software is theoretically so easy it has made software vulnerability the cornerstone of arguments for a return to hand-marked paper ballots.<sup>13</sup>

Various hacker sites now sell the tools needed to carry out voting machine attacks to anyone who wants to buy them. If you want to become a malicious hacker, it’s relatively easy to find online tutorials explaining how to assemble your own “rootkits.”

A rootkit is difficult-to-detect software that enables someone to take control of a computer from a remote location. For a few hundred dollars, anyone can acquire the means to take over someone else's computer system.

"It's just like purchasing software for a computer from Microsoft or Adobe — except that there's this criminal enterprise running the website," DeMillo joked.

Another type of hack is through SQL (Structure Query Language) injection. Anyone who has mastered the technology can modify databases, shut down administrative actions, and take remote control of a device.<sup>14</sup> As the 2016 election made clear, more than a few foreign actors find this kind of hacking perfectly acceptable behavior. Among the leaders in the field: Russia, China, and Iran.

### ***Does it take a great deal of technical experience to manipulate election equipment?***

The degree of expertise required depends on the type of attack, but it generally does not take a great deal of skill to attack a voting system.

Teenagers and even young children can have a field day on election equipment. The Voting Village events at the annual DEF CON meetings are often crowded with children interested in cybersecurity and how to defeat it. At the 2018 meeting, an 11-year-old participating in the competition hacked into a mock-up of Florida's election results website and changed its reported vote totals in less than 10 minutes.

We know that malicious actors are already capable of attacking voter registration systems in the United States. In Florida, for example, election officials learned that Russian hackers accessed at least two county governments' networks during the 2016 election.<sup>15</sup>

The Senate Intelligence Committee issued a massive report looking into the scope of Russia's interference; luckily they had found no evidence that the hack had gone further than some poking and prodding around. There was not enough information for the committee to determine whether voter registration databases were disrupted.<sup>16</sup> Nevertheless, the vulnerability of election systems in the United States was clear for everyone to see. At risk are not only the machines that record votes, but also the registration systems that determine which voters are authorized to cast ballots.

### ***How long would it take to discover that someone had disrupted a voting machine?***

It depends on the type of attack and skills of said attacker. If the malware operates as intended, it will never be detected.

When Logan Lamb, a cybersecurity expert, found a "Shellshock" virus in Georgia's election servers at Kennesaw State University, the first thing he noticed was that the attackers had returned and patched the vulnerability that enabled them to break into the system.

There was some cause for alarm because the vulnerability had appeared in the state's "My Voter Page."<sup>17</sup> The flaws in the security system were so pronounced that even a novice could have exploited Georgia's voter registration database, thus taking a roundabout path to influencing the election itself.

“It’s like a burglar breaking into an apartment,” DeMillo said. “Once they find the door open, they may shut the door behind them and lock the door so no one else can get in.”

### ***Are voting machines connected to the internet?***

The biggest concern among election security experts is the fact that many of these systems can be connected to the internet. Even an indirect connection is potentially dangerous.

When vendors say their machines do not have a “direct connection” to the internet, experts ask whether that is really true if a voting machine receives its programming from a central server. The server gets its programming from the internet, so unless election officials are careful about what gets transferred to a voting machine, malware or bad data may be introduced through an intermediary machine.

“It’s very hard to tell what election officials mean when they claim that machines don’t have internet connectivity,” DeMillo explained.

Technically, voting machines are not supposed to be connected to the internet. In reality, they have been and continue to be — even when the voting-machine vendors tell Congress the opposite.

In August 2019, *VICE News* reported that the top voting-machine companies have dozens of systems that connect to the internet:

Some of the systems have been online for a year and possibly longer. Some of them disappeared from the internet after the researchers notified an information-sharing group for election officials last year. But at least 19 of the systems, including one in Florida’s Miami-Dade

County, were still connected to the internet this week, the researchers told Motherboard.<sup>18</sup>

Voting-machine vendors vehemently insist that while their products may have had indirect connectivity in the past, that is no longer the case. But DEF CON hackers have proved that anyone with a few minutes to spare could secretly connect a voting machine to the internet through a USB port.<sup>19</sup> That person could then install malicious software remotely, change vote counts, and even turn the machines off.

One of Voting Village's co-founders, Harri Hursti, is especially concerned about the lack of coordination between election equipment vendors and officials.

"Right now, we don't even know how vulnerable these machines are," Hursti said. "It's dangerous to think that if you fix everything that [the Voting Village] found, it would be enough to be secure."

### ***How can e-poll books be manipulated to disrupt the voting process?***

While e-poll books can drastically reduce long wait times at polling places, serious problems may arise if there is no paper backup.

E-poll books can seriously impact an election if they are hacked or otherwise malfunction.

During DEF CON's 2019 Voting Village, for example, cybersecurity experts raised a number of concerns about e-poll books. Hackers were instructed to tinker with these machines and successfully manipulated them in just a few minutes. Some folks decided to turn their e-poll book into screens for video games.

Among the e-poll books examined was ES&S's ExpressPoll. The password that vendors had installed was the name of the manufacturer. In case anyone had difficulty guessing that, the programmers working for the vendors had left the password in plain text so that it could be discovered on the e-poll book itself.

Of course, e-poll books can be adapted to meet safety guidelines, but there are no uniform standards, and local election officials frequently lack the resources to do proper testing.

It's not necessary to falsify voter returns to disrupt an election. All a hacker has to do is trigger enough chaos to disrupt wait times so that voters either give up or are turned away. The check-in process, DeMillo suggests, is a major vulnerability because if you create impossibly long lines you are effectively denying people the right to vote. "People can't wait seven, eight, nine hours in line just to check in for voting," said DeMillo.

## WHICH STATES USE POSTELECTION AUDITS?



**CALIFORNIA**  
(OPTIONAL RLA)



**OREGON**  
(OPTIONAL RLA)



**WASHINGTON**  
(OPTIONAL RLA)



**NEVADA**  
(STATUTORY PILOT PROGRAM)



**COLORADO**  
(IN STATUTE)



**MICHIGAN**  
(ADMINISTRATIVE PILOT PROGRAM)



**INDIANA**  
(STATUTORY PILOT PROGRAM)



**OHIO**  
(OPTIONAL RLA)



**NEW JERSEY**  
(ADMINISTRATIVE PILOT PROGRAM)



**GEORGIA**  
(STATUTORY PILOT PROGRAM)



**VIRGINIA**  
(IN STATUTE)



**RHODE ISLAND**  
(IN STATUTE)

Source: <https://www.ncsl.org/research/elections-and-campaigns/risk-limiting-audits.aspx>

### ***Why are risk-limiting audits not always helpful?***

A risk-limiting audit (RLA) tells officials absolutely nothing about whether a DRE or BMD correctly recorded a voter's choices. The only thing it confirms is whether the reported outcome of an election matches the printed paper record.

Dr. Philip Stark, who invented the RLA, resigned from Verified Voting's board of directors after the organization partnered with Georgia in order to conduct a test RLA on the state's newly purchased BMDs. So did DeMillo, who was especially outraged that no one warned him in advance that the test audit was about to take place.<sup>20</sup>

Stark points out that a fundamental problem with DREs and BMDs is that only the voters know for sure whether the printouts match their votes, or whether they made mistakes. There is no feedback mechanism. If a vote is made in error, there is no way of proving whether the machine or the voter was at fault.

If a DRE with a VVPAT or a BMD records the wrong results, Stark said, "then checking the tabulation of the pile of paper doesn't say very much about whether the outcome of the election is right."

More than 1,000 Georgia residents filed a petition in 2019 after then-Secretary of State Brian Kemp approved Georgia's new touchscreen voting machines. Kemp, who was also running for governor at the time he was responsible for overseeing the 2018 election, refused to make documents for the certification process available to the public.

The equipment in question was Dominion's ImageCast X Voting System, which Georgia's state legislature had approved more than \$100 million to purchase.



Kemp finally released the documents to the public a year after he won the election and became governor. The election itself had been riddled with allegations of voter suppression. The documents Kemp released were also suspect. Crucial information was missing, including the name of the person who had supposedly overseen the state certification process for the new election equipment.<sup>21</sup>

In late 2019, government watchdog groups filed a new complaint with the new secretary of state, Republican Brad Raffensperger. This time nearly 2,000 signatures — which came from almost every county in Georgia — were on the petition. Even the Libertarian Party of Georgia joined in.<sup>22</sup>

Raffensperger's deputy, Jordan Fuchs, told *WhoWhatWhy* their office would comply with the legal requirements for reexamination, "but the activists requesting the reexamination will have to pay for it."<sup>23</sup>

When the machines themselves, as well as the officials overseeing the election, are suspect, an RLA may not do much to restore confidence.

Another limitation of the RLA is that it is only useful if there is a noticeable difference between totals in the returns. Mercuri thinks the RLAs may create a false impression.

"If they're one percent apart," she said, "you're going to have to count more ballots than if they were 10 or 20 percent apart. So what you're saying is, you're going to trust what the computer spits out as the disparity. We're not calculating the disparity, the disparity is being calculated by the voting machines that were counting the ballots."

Her main concern is that the formula relies on a number that could be incorrect. "You can't rely on that for the calculations," she said.

“It doesn’t address the problem of ballots being marked incorrectly, if there have been shifts that occurred in the voting equipment,” she added. “That’s not why I fought for over 20 years to get paper ballots, because the reason for the paper ballots was to be able to count the paper ballots — not to say we’re just going to count 16 of them and that’ll be fine.”

## Notes

1. Matt Blaze, Jake Braun, Harri Hursti, David Jefferson, Margaret MacAlpine, Jeff Moss, “[Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure](#),” DEF CON 26 Voting Village, September 2008.
2. “[Tamper-Indicating Seals: Practices, Problems, and Standards](#),” Los Alamos National Laboratory, 2003.
3. Gabriella Novello, “[Ignoring Warning Signs: Officials Approve Vulnerable Voting Machines](#),” *WhoWhatWhy*, January 6, 2020.
4. Gabriella Novello, “[Lawmakers Grill Voting Machine Vendors on Paperless Machines](#),” *WhoWhatWhy*, January 9, 2020.
5. Frances Robles, “[Nearly 3,000 Votes Disappeared From Florida’s Recount. That’s Not Supposed to Happen](#),” *New York Times*, November 16, 2018.
6. Rebecca Shabad, Shaquille Brewster, and Lauren Egan, “[Wisconsin voters face long waits, lines amid coronavirus outbreak](#),” NBC News, April 7, 2020.
7. Gabriella Novello, “[States Grapple With Germ-Ridden Voting Machines](#),” *WhoWhatWhy*, May 5, 2020.
8. “[Customer Notification: COVID-19 Information](#),” Dominion Voting, March 9, 2020.
9. “[Statement by NCSC Director William Evanina: 100 Days Until Election 2020](#),” Office of the Director of National Intelligence, July 24, 2020.
10. David Goldstein, “[Goldstein Investigation: Officials Warn Of ‘Vulnerabilities’ With E-Voting Machines Ahead Of March 3 Primary](#),” CBS Los Angeles, February 4, 2020.
11. Matt Blaze et al., “[DEF CON 27 Report](#),” Voting Machine Hacking Village, August 2019.

12. Kim Zetter, "[Software vendor may have opened a gap for hackers in 2016 swing state](#)," *Politico*, June 5, 2019.
13. Andy Jackson, "[The Only Safe Means of Voting is Hand-Marked Paper Ballots](#)," Civitas Institute, June 13, 2020.
14. "[SQL Injection](#)," Open Web Application Security Project, accessed April 2020.
15. Miles Parks, "[Florida Governor Says Russian Hackers Breached 2 Counties In 2016](#)," NPR, May 14, 2019.
16. "[Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures, Campaigns, and Interference in the 2016 US Election](#)," 116th Congress, 1st Session.
17. Jordan Wilkie and Timothy Pratt, "[Georgia's Voter Registration System Like 'Open Bank Safe Door'](#)," *WhoWhatWhy*, November 4, 2018.
18. Kim Zetter, "[Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials](#)," *VICE News*, August 8, 2019.
19. Matt Blaze et al., "[DEF CON 27 Report](#)," Voting Machine Hacking Village, August 2019.
20. Gabriella Novello, "[Divide and Conquer? Voting Machine Audit Causes Rift Among Experts](#)," *WhoWhatWhy*, January 22, 2020.
21. Gabriella Novello, "[Georgians Demand Secretary of State Re-Examine Voting System](#)," *WhoWhatWhy*, August 20, 2019.
22. Ibid.
23. Gabriella Novello, "[Georgia Demands Fee to Re-Examine Hinky Voting Equipment](#)," *WhoWhatWhy*, August 21, 2019.

5.

## SOLUTIONS AND GLOBAL PERSPECTIVES

---

### ***Why isn't voting "federalized"? What parts of it are?***

The US voting system is a gigantic patchwork of regulations that are not only different from state to state, but can also be different from one county to another. Counties, cities, and towns can and do set up their own rules that govern everything from the purchase of election systems to when and how voters register and cast their ballots.

It might make more sense to have one system that applies to everyone, but that is not likely to happen. "I guess the place to start ... is the Constitution," said Ben Hovland, head of the federal Election Assistance Commission (EAC).

A small, independent watchdog agency, the EAC was created as a result of the Help America Vote Act of 2002, which was itself a response to the controversy that focused on the Florida vote in the 2000 election. The EAC provides extensive guidance and help to the officials who run America's elections but has no authority to enforce its recommendations.

Hovland notes that several types of law do have an impact on federal elections. Amendments to the US Constitution expanded

suffrage — the right to vote — to African Americans, to women, and finally to 18-year-olds.

The Voting Rights Act was designed to counteract racial discrimination at the polls. The **National Voter Registration Act**, which came to be known as the “motor voter” law, was created to make it easier to register by authorizing state motor vehicle departments to register voters. The Uniformed and Overseas Citizens Absentee Voting Act enabled citizens living overseas and the military to cast absentee ballots. But Hovland insisted that apart from these exceptions, “federal legislation in this space is very limited.”

Hovland says he initially saw advantages in having the federal government standardize election laws, but he now thinks innovation at the state level can be more practical. For example, because the wheels of legislation move so slowly, Hovland says it would take a long time to enact a national mandate to check all election results with a risk-limiting audit (RLA). However, acting on its own, Colorado was able to pioneer its use of RLAs in the state. The federal government assisted Colorado with additional funding, and grant money was provided by the Help America Vote Act and the Election Assistance Commission. That enabled the state to get started.

Similarly, Hovland says that online voter registration began in Arizona, then spread to Washington, and as it became apparent that the approach was saving time and money, it spread quickly. “Now, 40 states have online registration, [so] there really are advantages to that ability to pilot, to innovate at the state level ... I think where the federal role comes in is [to] ensure that people’s right to vote is protected and there are [not] overly burdensome local laws or rules put in place,” he said.



Benjamin Hovland, commissioner of the US Election Assistance Commission.  
Photo credit: [EAC](#)

### ***How does US voter turnout compare with other countries?***

When it comes to voter turnout, the United States doesn't do particularly well compared to other nations.

The Pew Research Center, which has tracked US voter turnout for years, reports that the US places 26th on the list of 32 highly industrialized nations that are members of the **Organization for Economic Cooperation and Development**, or OECD.<sup>1</sup>

Pew found close to 56 percent of voting-age Americans cast a ballot in 2016's presidential election (even though pollsters noted that

70 percent of Americans questioned said they considered a “high turnout” to be very important).

The three highest-scoring nations on the list in 2016 were Belgium, Sweden, and Denmark. More than 87 percent of the voting-age population in Belgium, where voting is compulsory, turned out in 2014. Nearly 83 percent of voting-age people in Sweden showed up the same year, and around 80 percent in Denmark voted in 2015.

Toward the bottom of the list came nations such as Chile, which switched from compulsory to voluntary voting in 2013, although eligible citizens were still automatically registered to vote.

Pew notes:

In many countries, the government takes the lead in getting people’s names on the rolls — whether by registering them automatically once they become eligible (as in, for example, Sweden or Germany) or by aggressively seeking out and registering eligible voters (as in the UK and Australia) ... In the U.S., by contrast, registration is mainly an individual responsibility. And registered voters represent a much smaller share of potential voters in the U.S. than just about any other OECD country.

Before and after becoming president, Trump has repeatedly charged that the US voting system is rife with voter fraud despite the fact that copious published research suggests no evidence proving its widespread existence.<sup>2</sup>

Trump created the Presidential Advisory Commission on Election Integrity in 2017 with the stated goal of improving the American voting system and fighting allegedly widespread fraud. Government officials and civil rights watchdogs across the nation pushed back

hard, saying there was no proof of massive fraud and that it was outrageously invasive for the federal government to demand that states hand over detailed (and sometimes irrelevant) personal information about every voter.<sup>3</sup> The commission was disbanded after it found virtually no fraud and did almost nothing to improve the current voting system.

(As an aside, there's a difference in what's meant by "voter fraud" and "election fraud." According to *FindLaw*, the first encompasses shady practices such as voting under an address where you no longer live, selling your vote to someone else, or voting twice in the same election. The second is bigger than an individual act, such as faking the signatures required to get a candidate on the ballot, or "ballot harvesting," in which a third party collects and alters mail-in ballots before delivering them to be counted.<sup>4</sup>)

The coronavirus pandemic, which by mid-August 2020 had killed more than 170,000 Americans, raised questions about the safety of voting in person. One solution appeared to be widespread authorization of vote-by-mail. After telling a Fox News audience that vote-by-mail would probably permanently end any chance the Republican Party had of winning future elections, Trump launched a two-pronged attack against both the concept of vote-by-mail and against the US Postal Service itself.<sup>5</sup>

Trump then proceeded to dismiss the threat from the coronavirus pandemic, despite predictions at the time that it might kill as many as 200,000 Americans if not brought under control. In a characteristically self-contradictory tweet, Trump opined: "Absentee Ballots are a great way to vote for the many senior citizens, military, and others who can't get to the polls on Election Day" but he considered mail-in absentee ballots to be "very different from 100% Mail-In Voting, which is 'RIPE for FRAUD,' and shouldn't be allowed!"<sup>6</sup>



Nonetheless, the coronavirus pandemic could have a major impact on voter turnout in the November election, especially since the pandemic may become even more serious if another wave coincides with the fall flu season. On the other hand, a major shift to vote-by-mail could overload the system's current capacity to process mail-in ballots.

Other factors that could have an impact on voter turnout include: Voter ID laws, which require voters to show some form of picture identification or state-issued identification; the fact that Election Day is not a national holiday; long wait times at the polls; the absence of all-mail, early, and no-excuse absentee voting in many localities; challenges with transportation; and lack of access for rural and disabled Americans.

Then there's plain old apathy, or cynicism — a sense, depending on how deeply "blue" or "red" a voter's state may be, that an individual's vote really "doesn't matter."<sup>7</sup>



102-year-old Desiline Victor stood in line to vote for six hours in Miami in the 2012 presidential election. Victor is shown here receiving applause after being recognized by President Barack Obama during his February 12, 2013, State of the Union speech. Photo credit: [Ascender Films, Inc. / Vimeo \(CC BY 3.0\)](#)

### ***How can the voting process be streamlined and wait times minimized?***

It generally takes less than 10 minutes to cast a ballot in person; the time voters wait in line before being able to vote can be considerably longer.

Some voters are prepared to wait in line almost indefinitely in order to cast a ballot. Desiline Victor, at the age of 102, waited for hours in order to cast her vote for Barack Obama in the 2012 election.<sup>8</sup> Not all voters have the time, endurance, or inclination to wait that long. In a more perfect universe, they wouldn't have to.

Jeanette Senecal, senior director of mission impact at the League of Women Voters, suggests that long lines at the polling place are part of the explanation for why voting often takes longer than it should,

but those lines don't represent the whole story. "The Presidential Commission on Election Administration, launched by President Obama in 2013, set a benchmark of 30 minutes for wait times,"<sup>9</sup> Senecal told *WhoWhatWhy*. "Research has shown that the vast majority of voters wait 30 minutes or less, but there are polling places where voters wait an hour or longer.

"Lines are often a symptom of challenges," Senecal said. "Too few poll workers ... or too few voting locations for any one community, confusing polling place layout, e.g. multiple precincts in the same polling place with people waiting to check in at the wrong place. Some of the causes for long lines at polling places on Election Day include malfunctioning machines, missing ballots, if poll workers aren't ready, or there is just heavy voter traffic due to heightened interest in the election."

A 2016 study by the Brennan Center for Justice and entrepreneur Craig Newmark found that Millennial and Gen X voters were as much as four times more likely to have to wait in line at polling stations than Baby Boomers.

African Americans were four times likelier than white people to have to wait 30 minutes or more. Latinx voters were six times more likely than white voters to have to wait.<sup>10</sup> People of color and young voters often live and vote in underserved communities and have less flexibility concerning time than older white voters, who are more able to avoid rush hours at the polls.

The obvious solutions that seem to be gaining more currency, particularly in light of the coronavirus pandemic, are early voting and absentee voting.

"Early voting is a great way to avoid long lines on Election Day and participating in early voting also alleviates the pressure for voters

and poll workers,” Senecal said. “Every state now offers some form of early in-person or absentee voting, but this varies by state, some states require an excuse to qualify for absentee voting or they impose limited hours and locations for early voting.”

The National Conference of State Legislatures reports that at least 34 states and the District of Columbia currently allow “no-excuse” absentee voting under all circumstances.<sup>11</sup> That means voters can request a mail ballot without having to explain that travel, illness, or something else would prevent them from voting in person. Most of the remaining states that haven’t yet authorized no-excuse absentee voting are in the Northeast and the South.

### ***How can voters ensure that their vote is secure and counted?***

Senecal advises voters to take advantage of early and absentee voting opportunities, check their registration status well ahead of deadlines, bring proper identification to the polls in places where it’s required, and reduce the potential for confusion and mistakes by deciding whom and what to vote for ahead of time.

Hovland recommends going a step further. “I try to encourage people to serve as poll workers,” he said.

Hovland added that in some voting districts you can actually track your ballot the same way you would a parcel. Localities like Denver and Boulder County in Colorado have developed systems respectively called Ballot TRACE and Ballot Track. As Denver’s ABC affiliate described it ahead of the 2016 presidential election, Ballot TRACE “uses the U.S. Postal Service’s barcode technology to track a

ballot envelope from its printing, to its delivery to your home, and then back to the elections division after it is mailed back.”<sup>12</sup>

### ***How do Americans overseas, civilian and military, cast their votes?***

The Federal Voting Assistance Program (FVAP) “trains and supports over 3500 voting assistance officers across the military services and works closely with [the] State Department to educate and inform military and overseas citizens about the absentee voting process,” said the program’s director, David Beirne.

That doesn’t mean that FVAP is responsible for how each service member’s home state administers his or her ballot, Beirne explained. “Each state is responsible for authorizing the specific methods available for voters to receive blank ballots and return their voted ballots.” Additionally, “Under federal law, each state must authorize an electronic means of receiving a blank ballot, which is usually done by email or with a reference link to a website to retrieve the ballot.”

US military personnel can return ballots by mail, fax, or electronically.<sup>13</sup>

Overseas personnel can also use the Military Postal System Agency. Clerks of the MPSA, which is available at most military installations, use a special label to help speed ballots back to election officials. Overseas citizens not in the military are encouraged to drop their completed ballots off at their nearest embassy or consulate for return to the United States at no cost, Beirne says. They can also mail their ballots back to the US via a foreign postal service at their own cost.

To support stateside election officials in processing ballots from those who fall under the Uniformed and Overseas Citizens Absentee Voting Act, Beirne said FVAP puts a special emphasis on timing and encourages “military and overseas citizens to start their voting process early and complete the correct forms.” If a UOCAVA voter doesn’t get a ballot the usual way, the assistance program can provide a federal write-in absentee ballot (yes, there’s an acronym for that: FWAB), or one can be downloaded from FVAP’s website along with instructions.

FVAP serves members of the Army, Navy, Marine Corps, Air Force, and Coast Guard, as well as the United States Public Health Service Commissioned Corps, National Oceanic and Atmospheric Administration Commissioned Corps, Merchant Marines, and their eligible family members. FVAP also generally assists American citizens living outside the US.

FVAP estimates it serves about 1.3 million active-duty service members, plus another 700,000 spouses and dependents. (Note: FVAP only gets involved when the service member or dependent isn’t voting from the place where they are normally registered to vote.) In 2016, FVAP estimated that about 5.5 million US citizens were living overseas, and that at least three million were old enough to vote.

FVAP’s entire budget is around \$5 million, although that can fluctuate from year to year, Beirne said. That budget covers “personnel and outreach activities including updates to and maintenance of the FVAP.gov website, production and distribution of informational materials, training, social media, and research supporting program improvement and required reports to Congress.”

It may sound like a lot of money just for an election, but it is all relative. *Military Times* reported the Department of Defense recently spent \$4.6 million on... seafood. More specifically, “The Pentagon spent \$2.3 million on crab, including snow crab, Alaskan king crab, and crab legs and claws, as well as another \$2.3 million on lobster tail.”<sup>14</sup>

### ***What is the past, present, and future of online/app voting?***

Online voting has a long way to go before it is a genuinely viable option.

Researchers at MIT and the University of Michigan gave bad news concerning online voting in a June 2020 report, which declared that

online ballot return ... represents a severe danger to election integrity and voter privacy. At worst, attackers could change election outcomes without detection, and even if there was no attack, officials would have no way to prove that the results were accurate.<sup>15</sup>

This particular study focused on Democracy Live’s OmniBallot platform, which voters can use in states such as Delaware, New Jersey, and West Virginia.

As one of the study’s authors, Michigan’s J. Alex Halderman, explained in a series of tweets,<sup>16</sup> the OmniBallot platform can be used in three ways: Voters can print, mark, and mail their ballots; mark them online and mail, email, or fax them in; and in some states, directly cast votes online.

“States are adopting OmniBallot for laudable reasons: to help overseas voters, voters with disabilities, and those who can’t safely go to the polls due to COVID-19,” Halderman explained. “But, as we learned in 2016, elections face serious security threats. That’s especially true for online voting.”

Adding to the fact that OmniBallot appeared vulnerable to malware that could be used to manipulate votes, the researchers noted that

Democracy Live, which appears to have no privacy policy, receives sensitive personally identifiable information — including the voter’s identity, ballot selections, and browser fingerprint — that could be used to target political ads or disinformation campaigns.

Halderman, explaining the findings, said there is no really secure way to give the public online voting with the technology we have right now. He noted that, “The National Academies and the Senate Intelligence Committee both urge against using it, even for military voters.”<sup>17</sup>

“Bottom line,” tweeted Halderman, “OmniBallot’s ballot delivery and marking can be valuable tools for helping voters participate \*if\* officials take the precautions we suggest. Online voting, however, is a severe danger to election integrity and privacy, and we urge jurisdictions not to deploy it.”

Experts point out that a secure connection to a server doesn’t necessarily mean a secure vote: A botnet, or a system of “connected computers performing a number of repetitive tasks,”<sup>18</sup> can change votes between the time they’re cast and received, potentially without detection.



Verified Voting, a nonpartisan nonprofit dedicated to supporting accurate, transparent elections, warns that “there is no effective way to prevent such an attack, and no effective recovery.”

The “secure” transactions that might offer a path to online voting aren’t foolproof. News stories about major data breaches of retailers, credit card companies, and social media hubs are so frequent that they barely register as news these days. Verified Voting points out, “People have the illusion that ecommerce transactions are safe because merchants and banks don’t hold consumers financially responsible for fraudulent transactions that they are the innocent victims of.”<sup>19</sup>

If major banks can’t prevent cyberattacks, how will understaffed, underfunded town boards of elections be able to do so?

### ***Is there a movement to return to hand-marked paper ballots?***

Proponents of using hand-marked paper ballots cite a slew of practical reasons to use them. First, they create a physical paper trail that can’t disappear if a voting machine malfunctions: The ballot can be saved, reviewed, and counted again in an emergency or in an audit to confirm the outcome of an election. Second, voters don’t have to be tech savvy to read or complete them.

Marking by hand, of course, isn’t a panacea for problems with our election equipment. Hand-*marked* doesn’t necessarily mean hand-*counted*, for one thing: There can still be machines involved in the tabulation process, and they can still malfunction. Also, hand-marked ballots are famously prone to ambiguity. If a ballot calls for filling in an oval next to a candidate’s name, and a voter does

something else — underlines the name, circles it, puts a check mark next to it — does that count?

Amber McReynolds, CEO of the National Vote At Home Institute and Coalition and former Denver director of elections, notes that the problem with hand-marking ballots is that not everyone can use them. Setting up a situation where people need to make special requests in order to vote comfortably, accurately, and privately can be a slippery slope, particularly if it means requiring that someone disclose a disability.

Hand-marking, McReynolds says, just isn't for everyone. Personal example: "My mom, she has arthritis very bad in her hands... I've seen her try to fill in ovals, like they're light and it's hard, [and] I don't think it's fair to her [for me] to say, 'Well, let me help you.' She should have an independent experience. And so, I think the future is options for voters. And what I mean by that is ... if you need a remote, accessible vote-by-mail option at home, we need to be able to provide that for you. We need to figure out the security, we need to figure out the platform," she said.

Is that practical? "There have been some advancements... California has a remote, accessible vote-by-mail process. You still print the ballot at the end. It's not transmitted electronically back, but you get your ballot, you mark it on your screen or your equipment at home, you print it out, and you return it," McReynolds said.

Whether voting remotely or at a polling place, when it comes to hand-marked paper — or even whether to push for all-mail voting or voting in person — McReynolds, for one, doesn't espouse a one-size-fits-all approach. That could mean letting people vote by mail, with a ballot-marking device if they need one, or fill out ballots at home and drop them off, or vote at a traditional polling place. "To

me, giving voters all the options to choose from, that's what we should be doing at home or in person."

***Do rhetorical threats undermine confidence in elections, regardless of how good (or bad) technology is?***

Technology isn't everything when it comes to voting: Trust in the system also matters.

Well before he was president, Donald Trump sought to cast a shadow over the trustworthiness of the election he was trying to win. In 2016, while there were real threats to the integrity of the election system, Trump was on the stump with a message: The election might be "rigged" in favor of his opponent, Democrat Hillary Clinton.

His messaging raised red flags:

There is no evidence of full-scale or widespread voter fraud, and I think it's very unfortunate to suggest to supporters that might be the reason you would lose [an election], rather than it be the personal responsibility of the candidate to not have been able to persuade enough voters to vote for him or her

said Fox News host Dana Perino, who had previously served as George W. Bush's White House press secretary. Perino made the remarks when she appeared on an October 2016 episode of the podcast *Special Relationship*. Her observations made sense, but Trump was not alone in raising suspicions about election integrity.<sup>20</sup>

A few days before the 2016 election, a survey by Rad Campaign and Lincoln Park Strategies found that a hefty 40 percent of millennials

did in fact believe the election could be “rigged.” Overall, *Mic* reported,

Despite reams of evidence that counter the idea that sporadic attempts to game the election system are actually an epidemic, more than a third, 36 percent, of the 1,109 Americans in the poll told researchers they believe a single party or candidate could wield the power to fix the outcome.<sup>21</sup>

(Just *how* the rigging would work ended up splitting the poll respondents. Some thought it would be voter suppression that could skew the results, while others said it would be voter fraud.)

More recently, 2020 Democratic presidential nominee and former Vice President Joe Biden has raised the question of what would happen if Trump refused to accept defeat in his reelection bid. Biden said in a June appearance on *The Daily Show* that the possibility that Trump would “try to steal this election” was his “single greatest concern.”<sup>22</sup> (Biden didn’t specify how the incumbent might pull that off, but did say he’d considered a dystopian scenario in which Trump refuses to part with the Oval Office and has to be escorted out by the military.)

So while legitimate threats to the machinery and system of voting exist in the US, both major candidates have spent time conjuring up the specter of an election that in some undefined, unproven way, isn’t completely legitimate. Trump, on balance, appears to have spent much more time raising ungrounded fears that active fraud could throw the election (by people fiddling with mail ballots, or voting on behalf of the dead, or via ballots cast by undocumented immigrants... the list really does go on).

Senecal cautioned, “Speaking negatively about voting is known to discourage voters from even wanting to participate in elections. Talking about barriers and challenges or how hard it is going to be in order to vote can turn voters off. Language around elections being ‘rigged’ or ‘voter fraud’ undermines the integrity of our elections and hurts voter confidence.”

### ***What legislation could be considered or passed to make voting better?***

The Protecting American Votes and Elections Act of 2019, which Sen. Ron Wyden (D-OR) introduced with 14 co-sponsors, mandates paper ballots and risk-limiting audits for federal elections to protect against and detect outside interference in voting.

Additionally, HR 1, which House Democrats passed in March of 2019, “is aimed at getting money out of politics and increasing transparency around donors, cracking down on lobbying, and expanding voting rights for Americans by implementing provisions like automatic voter registration,” as *Vox* reported.<sup>23</sup>

McReynolds told *WhoWhatWhy* that she sees a number of other measures that could improve American voting.

“I think one of the simplest ways that they could solve a whole lot of problems right now ... [is] just to pay for postage like they do for military ballots,” she said. “Military ballots have a federal indicia. The postage is paid by the federal government. It automatically gets charged to the federal government when every jurisdiction in the country uses the same indicia. And I think they should apply that to all domestic ballots, and that would immediately take some of the

financial burden of mailing out ballots that falls on localities right now off of them.”

Additionally, she says she finds it “kind of unbelievable” that states like Indiana still require the average person to prove they have a specific reason to need to vote absentee besides simply wanting to do so. (One of the qualifications for an absentee ballot, she noted, is being categorized as a “serious sex offender” under Indiana law.)

Third, McReynolds said, “overcomplication of ballot styles generally can be really problematic when it comes to voter privacy,” especially when few people participate because of low party membership or weak turnout. “By streamlining and taking out some of that complication, we would protect voters’ privacy.”

### ***How do other countries compare to the United States?***

The major contrast between US systems and those used in other countries is not the type of machinery used to collect and tabulate ballots but the context in which it’s done. That’s according to Michael Yard, a senior global election technology and cybersecurity adviser with the International Foundation for Electoral Systems who has worked on elections from Azerbaijan and Cambodia to Kenya, Peru, and Sri Lanka.

“The biggest difference is that there’s no centralized system,” Yard told *WhoWhatWhy*. “I mean, every other country that I know of has one body that oversees and manages elections for the whole country, and we’re dissolved down to states and counties — [in America], everybody does it their own way.”

(Another major difference: Some nations either make voting mandatory or aggressively seek out and enroll citizens to vote. The United States does neither.)

In the Philippines, for example, election officials use ballot scanners to count votes, while in India, they have “a very simple hardware ... There’s no screen; you just punch a button and then the machines tabulate and send to a central counting and consolidation system,” Yard said. “Very simple. Nice hardware, nice system — except absolutely 100 percent opaque.”

Meanwhile, “Estonia has Internet voting and even some mobile phone voting. There are a couple of other countries that have done some experiments with Internet voting, but none that have been completely successful.”

Yard noted that Estonia, with a population of just over a million people, has “a long, slowly evolving history of digital identification. Everybody has a smart card for everything,” he said. “So they’ve got the infrastructure to manage it, and even with that infrastructure, a number of people have pointed out security holes in the Estonia system.”

Despite the potential vulnerabilities, “Estonians seem to have confidence in the system, and there is no evidence that it has been successfully attacked,” he said. Yard nevertheless added a note of caution: “A really successful attack would leave no evidence,” he says.

Yard also highlights Brazil as a successful example of a country deploying fairly sophisticated touchscreen voting machines. “I think the machines have major security issues,” he said, “but because the elections are completely controlled by the judiciary and voters have

high confidence in the impartiality and the integrity of the judiciary, everybody seems to be happy with that.”

Even though a relatively small number of manufacturers dominate the American market, the United States is forced to deal with a wide range of aging equipment and designs, the result of purchasing decisions made at different times by election commissions in different states and localities.

Systems used in the US run the gamut from basic to sophisticated, Yard said. “By far, my preference [is] ballot-scanner-type systems, because you end up with paper that you can audit later [and] you get the speed and efficiency of automatic counting.” Yard cautioned that even these systems have potential risks.

### ***Which country has the most efficient system?***

Yard says that several countries stand out with voting systems that not only provide accurate results, but also feature multiple layers of transparency so the public can see the process in as much detail as they want.

Here’s how he explains the system used in Kenya, which he called impressive — although, he added, “I’m not sure that I would want the U.S. to emulate full biometric systems and biometric verification of a voter on Election Day, but they [have] this in place.”

On Election Day in Kenya, voters show up at their polling place and touch a machine, which looks up their identity and confirms if they’re allowed to vote there. Then the voter receives and hand-marks the ballot.



At the end of voting, “they open the ballot box and they do the full manual count in front of all of the party agents and observers.” When the count is complete, election officials complete a “results protocol” form and photograph it. The photo is shared with political parties and on a public website where anyone can see the results from individual polling stations, and the results are sent to a central tabulation system to determine who won.

Because of the many specific layers of disclosure involved in how Kenya runs its elections, Yard said, “it’s a really good and transparent and accountable system.”

Yard also thinks the system used in the Philippines has strong points. After voters are checked in, their manually marked ballots are fed into a scanner which tabulates their choices. “Every polling station you go to has the exact same system, [and] they’re manned by BEIs, Board of Election Inspectors. [The] polling workers essentially are mostly teachers, so they’re all familiar with the process.”<sup>24</sup>

### ***What are nations where election tampering has occurred, and what can we learn?***

Setting aside what President Trump has insinuated about “rigged elections” in the United States (including the one he won in 2016), the truth is that real rigged elections have been documented many times in modern history.

Take the Philippines under Ferdinand Marcos, for example. After decades of dictatorial rule, including years of rule under martial law, Marcos “defeated” the opposition candidate, Corazon Aquino, in a 1986 “snap presidential election.”

As *Rappler* has reported,

The snap polls in 1986 were marred by reports of cheating, violence, and disenfranchisement of voters. The Commission on Elections (Comelec) declared Marcos the victor, but the National Citizens' Movement for Free Elections (Namfrel) said Aquino was the real winner, based on its own quick count."<sup>25</sup>

Shortly after the vote, with the dictator's win questioned both inside the country and out, including by the Reagan Administration, the Marcos regime was finally toppled in what became known as the People Power Revolution.

In another revolutionary case, Serbian strongman Slobodan Milosevic fell from power amid civil unrest after a 2000 election in which he claimed victory over Democratic Opposition standard-bearer Vojislav Kostunica.

The 2014 presidential election in Romania was marred by allegations that bribes of food were employed to influence the outcome. The Associated Press reported in 2016 that a court had "upheld the prison sentence of a former Romanian lawmaker known as 'the chicken baron' who was convicted of bribing voters with 60 tons of packaged, ready-to-fry meat."<sup>26</sup>

And Kenya's 2017 vote for president was annulled amid sharp questions about election irregularities; accusations of fraud "set off protests across Kenya, resulting in the deaths of at least 25 people, including a 6-month-old baby."<sup>27</sup> (The *New York Times* noted that in that year, the death toll was "far lower than in previous elections.")

All this is not to cast stones, by the way. The US is not immune to “rigged” or problematic elections. Take Lyndon B. Johnson’s 1948 run for Senate, just to name one: Per *Time*,

According to the account by Johnson biographer Robert Caro, the future president won a runoff primary by a mere 87 votes, after 200 extra votes were added to what Foley calls “the infamous Ballot Box 13.”<sup>28</sup>

What can we learn? The big takeaway is pretty obvious: Elections in the modern world can be, and are, not just vulnerable and problematic, but in fact rigged. The other lesson: When the public learns (or is convinced) that its will has been subverted, people will take action, from protests and revolution to even murder.

## Notes

1. Drew DeSilver, [“U.S. trails most developed countries in voter turnout,”](#) Pew Research Center, May 21, 2018.
2. [“Debunking the Voter Fraud Myth,”](#) The Brennan Center for Justice, January 31, 2017.
3. Celeste Katz, [“New lawsuit claims Trump’s ‘voter fraud panel’ violates the Watergate-era federal Privacy Act,”](#) *Mic*, July 14, 2017.
4. [“What Is Electoral and Voter Fraud?,”](#) *FindLaw*, March 18, 2020.
5. Paul Steinhauser, [“Trump says surge in voting by mail his ‘biggest risk,’”](#) Fox News, June 19, 2020.
6. Donald J. Trump, [Twitter Post](#), April 8, 2020, 7:34 PM.
7. [“On The Sidelines Of Democracy: Exploring Why So Many Americans Don’t Vote,”](#) *Morning Edition*, NPR, September 10, 2018.
8. Erika Bolstad and Nadege Green, [“First Lady invites 102-year-old North Miami woman to State of Union speech,”](#) *Miami Herald*, February 11, 2013.
9. [“The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration,”](#) January, 2014.

10. Celeste Katz, "[New Report Shows Millennial and Minority Voters Face Huge Obstacles at the Polls](#)," *Mic*, March 28, 2016.
11. "[Voting Outside the Polling Place: Absentee, All-Mail and other Voting at Home Options](#)," National Conference of State Legislatures, July 10, 2020.
12. "[Residents of Denver and Boulder counties can track their ballots online every step of the way](#)," ABC Denver7, October 20, 2016.
13. "[How Voters Can Submit Their Federal Post Card Application](#)," Federal Voting Assistance Program, last revised November 25, 2019.
14. Kyle Rempfer, "[Use-it or lose-it: DoD dropped \\$4.6 million on crab and lobster, and \\$9,000 on a chair in last-minute spending spree](#)," *Military Times*, March 12, 2019.
15. Michael A. Specter and J. Alex Halderman, "[Security Analysis of the Democracy Live Online Voting System](#)," MIT and University of Michigan, June 7, 2020.
16. J. Alex Halderman, [Twitter Post](#), June 7, 2020, 8:17 PM.
17. J. Alex Halderman, [Twitter Post](#), June 7, 2020, 8:19 PM.
18. "[What is a botnet?](#)," Malware, Norton, accessed June 2020.
19. David Jefferson, "[If I Can Shop and Bank Online, Why Can't I Vote Online?](#)," Verified Voting, 2014.
20. "[Rigged Election Realities](#)," Special Relationship, *Mic* and the *Economist*, October 28, 2016.
21. Celeste Katz, "[Nearly 40 percent of millennials in one survey say they believe the election could be rigged](#)," *Mic*, November 4, 2016.
22. Rebecca Shabad and Marianna Sotomayor, "[Biden's biggest fear: This president is going to try to steal this election](#)," NBC News, June 11, 2020.
23. Ella Nilson, "[House Democrats just passed a slate of significant reforms to get money out of politics](#)," *Vox*, March 8, 2019.
24. Sofia Tomacruz, "[Over 500,000 teachers to serve as poll workers on May 13 — DepEd](#)," *Rappler*, May 10, 2019.
25. Michael Bueza, "[Marcos vs Aquino, and past snap elections around the world](#)," *Rappler*, February 6, 2015.
26. "[Romania: court affirms prison term for chicken bribes](#)," Associated Press, March 17, 2016.
27. Kimiko de Freytas-Tamura, "[Kenya Opposition Leader Says He'll Expose Election Fraud](#)," *New York Times*, August 16, 2017.
28. Lily Rothman, "[Has an Election Ever Been Rigged in U.S. History?](#)," *Time*, October 19, 2016.

6.

## CONCLUSION

---



Photo credit: [Seattle Municipal Archives / Flickr \(CC BY 2.0\)](#)

American voting has come a long way from the simple wooden ballot box. Despite modern equipment, voters still want many of the same things that they have always expected in an election: a system that protects the secrecy of the ballot without concealing the process, and a system that guarantees their vote is faithfully reported and safe from outside tampering.

This book has focused on how a tiny group of manufacturers has managed to gain control over the tools which we Americans use when we cast a ballot.

Given what is at stake, the entire system — procurement, operation, and maintenance — would benefit from more transparency.

Every business seeks to maintain a competitive edge over competitors and to safeguard its intellectual property rights. Voting-machine manufacturers are no different. However, when the future of the nation is at stake, it is reasonable to expect that these companies comply with existing laws that require transparency and forbid conflicts of interest.

Manufacturers and governments need to work together to make the election process as transparent and credible as possible. Rules governing procurement bids need to be clear to everyone. Officials should be prevented from signing contracts if they can't explain and clearly justify their decisions.

There is no question that the market could benefit from more competition, although some advocate for more centralized federal control of our voting apparatus. Ideally, more players would speed innovation and reduce prices both for machines and for the software needed to operate them. Increased competition could also

motivate these companies to manufacture systems that are easier to use and ballots that are easier to read. Ballot scanners also need to be improved.

It makes sense to involve manufacturers in the regulation process, but only if government officials are able to make decisions according to their best judgment, and not by transferring their responsibilities to industry lobbyists.

Allowing the manufacturers to dominate the discussion is not in the public interest. All Americans should have access to the technical specifications of voting machines and which officials are involved in the industry. The future of the country depends on how this system works, and its operation needs to be transparent.

Manufacturers should be required to fully disclose their lobbying activities and campaign donations. Any company that refuses to be transparent should be sanctioned.

Clearer and stricter rules are needed to fully clarify the relationship between manufacturers and the officials in charge of purchasing these machines for the public. Reporting of personal financial relationships, such as “consulting” and “advisory” work performed by election administrators for the Big Three manufacturers, should be required legally, with substantial penalties for any violations so that the public can be made aware of any undue influences.

There has been a growing movement for hand-marked paper ballots in lieu of the vulnerable voting machines discussed in this book, largely because it is impossible to hack a piece of paper. Such a system is not without flaws, however. It could work in smaller jurisdictions, but it may be impossible in larger districts. Some voters are not able to complete a paper ballot with a pen or pencil. It takes time to process paper ballots, even using high-speed

scanners; voters, candidates, and even major news networks grew frustrated with the lack of instantaneous results during the 2020 primary election cycle because election officials could not immediately provide a final tally of absentee ballots.

The time has come for voting-machine vendors to make their machines more accessible.

That means pulling back the curtain and allowing cybersecurity experts in. As in any other industry, companies do not want their competitors to see how their products are made. But this is not just any industry. Voters must have a safe and secure way of casting their vote so they can elect the candidates that they want to office. Vendors could provide an appropriate avenue for outside experts to conduct security tests on their equipment every so often, then submit a confidential report explaining how they can improve.

And, if the United States does move toward hand-marked paper ballots or mail-in voting, voting-machine vendors can ensure that the equipment they provide for counting ballots is as up-to-date as possible. That starts with vendors offering to replace out-of-date and provenly vulnerable infrastructure with the most recent models of election equipment without placing an unnecessary burden on election officials.

When it comes to counting the vote, election officials should ensure that the software in optical scanners and e-poll books is also in prime condition. Voting-machine vendors, especially ES&S, claim that their equipment cannot be connected to the internet — even indirectly. But, as we've explained, this is not always the case. If vendors want to finally put this argument to bed, they could provide proof that their equipment is indeed "air-gapped." This means that there is a security network in place that prevents any unsecured connections to the internet in order to prevent hacking.



Electronic voting machines have flaws, but the likelihood of election officials being willing to scrap these machines for a paper-based system is slim (especially so close to the contentious 2020 election). Implementing mandatory postelection audits is one way to ensure that election results are as accurate as possible. At least 24 states are expected to have a postelection audit requirement in place before the November election.<sup>1</sup> It is not something that requires legislation, either. In fact, any local elections board can announce and conduct an audit before the results need to be certified.

Beyond our own borders, US election authorities can learn from the experiences of other countries when it comes to fair, accurate, and secure voting.

That can include regulation of the purchase and deployment of voting machines, the transparency of the counting and reporting of votes, the prevention of confusion and political pressure at poll sites, and the testing of systems that combine the ease of digital equipment with paper trails that are easy to trace and make public. This could also include an overall move toward systems that make voting and reporting the results easier, faster, and more accessible — and working with civic groups to ensure that's the case.

Voting is a unique activity, both from a theoretical and technical perspective. The machines and computer systems we use to run modern elections are complex, expensive... and vulnerable.

Realistically, it is not possible to abandon the new machines and implement hand-marked paper ballots nationwide — there is neither the time nor money for that — but better information about how operating limits are likely to affect machines needs to be made available, especially to election officials deciding on future purchases.

While you can't put a price on democracy, voting machines do have a price. As with any other business, the public should know what they're getting for their money.

## Notes

1. Andrea Cordova McCadney, Elizabeth Howard, and Lawrence Norden, ["Voting Machine Security: Where We Stand Six Months Before the New Hampshire Primary,"](#) Brennan Center for Justice, August 13, 2019.

7.

## ADDENDUM: IS MAIL-IN VOTING THE ANSWER?

---

### Introduction

Vote-by-mail has become an increasingly large factor in current American voting and will become historically significant in 2020, due to the coronavirus. In addition to the vulnerabilities within voting machines across the country, accessibility issues, and the murky money trail from the free market to our public servants, we also have a global pandemic to contend with. Public health and safety are of utmost concern in the 2020 election and perhaps will remain precarious in future elections. Due to this, activists, citizens, and some politicians are calling for a universal, no-excuse-needed vote-by-mail option. This would mean that every registered voter would get a mail-in ballot to fill out at home, to be submitted using a drop-off box or the US Postal Service. This method is not perfect. Tallying votes from absentee ballots takes a lot longer than in-person ballots — electronic or otherwise. There are also issues of how to securely store and seal the ballots, and how to ensure they are counted when the time comes.

*WhoWhatWhy* has been following this topic closely this election season. In this section, you'll find summaries of helpful vote-by-mail articles that delve into the details and the controversy of this new option.

## How Vote-by-Mail Became Another Partisan Fight

Before we begin, let's get one thing straight: absentee voting and mail-in voting are effectively the same thing, because voters are submitting their ballots through the mail instead of doing so in person. Lawmakers, members of the press, and voting-rights advocates use these terms interchangeably when talking about the process of filling out a paper ballot and returning it in the mail or at a ballot drop-off location. The only significant difference is that in a universal vote-by-mail system, election officials automatically mail registered voters a ballot.

It is unlikely that the coronavirus will magically disappear before the November election. What is certain is that, according to public health experts, *all* voters — Democrats, Republicans, and independents — put themselves at a significantly higher risk of contracting the virus if they spend hours waiting to cast a ballot in person. This is why so many states are choosing to offer mail-in voting at a level we have never seen before. Voting by mail is a must this November, but there are several forces trying to undercut this movement. Voters will be asking why, and many will be looking to their elected officials for answers. The motives behind opposition to mail voting, for many politicians, are already clear; as Trump himself admitted on *Fox & Friends* in March, “if you ever agreed to it, you’d never have a Republican elected in this country again.”<sup>1</sup>

The politicization of vote-by-mail reached a fever pitch when Wisconsin’s Democratic Gov. Tony Evers announced in an executive order that there would be an extension to postmark a mail ballot for the state’s April 7 presidential primary. The Republican-held state legislature successfully filed a lawsuit to block his executive order,

and millions of voters were forced to cast a ballot in person because they could not postmark a ballot before the deadline.<sup>2</sup>

Likewise, Kentucky's Republican Secretary of State Michael G. Adams pushed back against lifting certain restrictions to absentee voting. In mid-May, Adams told NPR that he wanted to expand access to vote-by-mail. Kentucky state law, however, requires that voters include a copy of their photo ID when they return a completed ballot. There is also a limited number of excuses allowed in order to request a mail-in ballot. As of July, there are two lawsuits to remove these requirements that are awaiting a lower court decision.<sup>3</sup>

Republican-backed groups have taken a keen interest in limiting access to nontraditional voting methods. Judicial Watch, a conservative and self-described "election integrity" group, filed a federal lawsuit in mid-April to purge nearly one million names from North Carolina's voter rolls. The lawsuit came less than 24 hours after the executive director of the state's Board of Elections, Karen Brinson Bell, requested that lawmakers consider expanding access to mail-in voting and allowing a utility bill as proof of identification.<sup>4</sup>

One daunting complication in the debate over vote-by-mail is the effort to defund the United States Postal Service, which is responsible for delivering absentee ballots in a timely manner. The Trump administration has repeatedly attacked the Postal Service, and President Trump reportedly threatened to veto any legislation to revive an agency that is effectively on life support.<sup>5</sup>

Concerns that an inadequately funded Postal Service will result in an election meltdown seem increasingly well founded. Louis DeJoy, a Trump-appointed postmaster general who began his term in June 2020, laid out plans to delay mail service in order to cut costs. That, compounded by declining revenue as fewer Americans use the

Postal Service, could cause a serious delay in transporting mail-in ballots this November.<sup>6</sup>

Another concern heading into November is the running theme among critics of mail-in voting that it will result in widespread voter fraud. To be clear, there is no evidence to support the notion of widespread voter fraud.<sup>7</sup> A person is more likely to be struck by lightning than engage in voter fraud. Despite this, a congressional panel in June showed just how severe the divide is on this particular issue. J. Christian Adams, president and general counsel for the Public Interest Legal Foundation — a conservative group known for suing state and local governments to purge voters from election rolls — told lawmakers on the House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties that a vote-by-mail system “is the most vulnerable form of voting.”<sup>8</sup>

Keeping up with President Trump’s Twitter feed and public statements regarding vote-by-mail may also seem daunting, but it is important to do so because we have already seen the impacts of his comments.

In 2018, Michigan voters passed a ballot initiative allowing any voter to cast an absentee ballot without providing an excuse. In May, Democratic Secretary of State Jocelyn Benson announced that she would mail absentee ballot applications to the state’s 7.7 million registered voters. Trump took to Twitter to falsely accuse Benson of mailing absentee ballots, eventually posting a new tweet to criticize her for doing what she actually had done: mail ballot requests, not the actual ballots.<sup>9</sup>

It is no secret that mail-in voting systems are not perfect — tens of thousands of voters in New York did not receive their absentee ballots in time to vote during the June 23 primary election.<sup>10</sup> The problem with Adams’s characterization, however, is that it suggests

the problem is not fixable. Local election officials have raised concerns about whether there are enough resources to process the likely surge in mail-in ballots. Increasing federal funds to keep the Postal Service running at full capacity could help minimize instances of voters not receiving ballots or ballots being discarded due to being received past the deadline (despite on-time postmarking). Hundreds of thousands of voters have requested a ballot already, and the Lawyers' Committee for Civil Rights Under Law rolled out an interactive online resource for voters to learn more about their state election laws.<sup>11</sup>

In addition to administrative shortcomings, voting-rights groups are also preparing for situations where election equipment fails to accurately record absentee ballots. What we saw in Georgia, for example, gave standing to this concern. Hundreds of ballots marked with 'X' or check marks were misread. Some races on the ballots were counted as non-votes.<sup>12</sup> This happened despite state law requiring voter intent to be considered when a ballot is reviewed. State election officials decided the errors were the fault of voters, but in the event that it was a programming error with the optical scanners, the problem is likely to be exacerbated when the machines are used to count millions of ballots this November.

### **Calling All Newsrooms: Get Ready to Not Report the Final Results on Election Night**

Journalists and newsrooms across the country must accept the fact that the final election results will not be ready in a few hours, days, or perhaps even weeks. With that in mind, there is still time to plan responsible coverage of the 2020 election (that means finding an alternative to reporting on exit polls, because far fewer voters will cast a ballot in person on Election Day).

Take it from Matt Hall, president-elect of the Society of Professional Journalists and editorial and opinion director for the *San Diego Union-Tribune*:

You can't just have the polls close at 8 o'clock and have a winner announced when the early results are in. I think everyone is going to have to kind of get used to ... [the fact that] elections are not drive-thru restaurants. We need to get it right, and sometimes that means waiting.<sup>13</sup>

Reporters have a responsibility to their readers. Voters need accurate information about the many changes taking place this year, including everything from what they need to bring to their polling place for proof of identification to how they can cast an absentee ballot if they prefer voting at home. Our advice? Explanatory journalism is the way to go this election cycle — and that should begin now, if not already.

## Mail-in Voting Explained

This is why *WhoWhatWhy* decided to launch “America Decides 2020” — a series that dives into the critical issues concerning who can vote, how ballots will be cast, and how they will be counted.<sup>14</sup> As part of our series, we answered some of the most common questions regarding voting by mail. What is the difference between mail-in and absentee voting? How does mail-in voting work? How can a voter submit an absentee ballot? Does voting by mail present a risk of widespread voter fraud?

It is vital that newsrooms make clear that absentee voting and mail-in voting are effectively the same thing — and we are emphasizing this point for a reason. President Trump has attempted to claim otherwise, tweeting that absentee voting is “very different from



100% Mail-In Voting, which is ‘RIPE for FRAUD,’ and shouldn’t be allowed!”<sup>15</sup>

Note that he said “100% mail-in voting,” which is also called universal mail-in voting. Under these circumstances, states automatically mail registered voters a ballot. California, Colorado, Hawaii, Nevada, Oregon, Utah, Vermont, Washington, and the District of Columbia will be doing that this year.<sup>16</sup> Some of these states have used this method of voting for decades.

## Notes

1. Darlena Cunha and DonkeyHotey, “[Mail-in Voting Is a Must This November](#),” *WhoWhatWhy*, July 5, 2020.
2. Gabriella Novello, “[How Vote-by-Mail Became Another Partisan Fight](#),” *WhoWhatWhy*, April 20, 2020.
3. Gabriella Novello, “[Kentucky Official Calls for Mail-in Voting, Limits Who Can Vote Absentee](#),” *WhoWhatWhy*, June 3, 2020.
4. Gabriella Novello, “[GOP’s Response to Vote-by-Mail: More Voter Roll Purges](#),” *WhoWhatWhy*.
5. Gabriella Novello, “[Activists Vow to Protect USPS as States Expand Mail-in Voting](#),” *WhoWhatWhy*, April 23, 2020.
6. Gabriella Novello, “[US Postal Service’s Ability to Deliver in November Questioned](#),” *WhoWhatWhy*, July 25, 2020.
7. Gabriella Novello and Erika Smithson, “[No, Voting by Mail Is Not ‘Ripe for Voter Fraud’](#),” *WhoWhatWhy*, April 29, 2020.
8. Gabriella Novello, “[Fear of Potential Vote-by-Mail Fraud Sparks Clashes Between Voting-Rights Groups](#),” *WhoWhatWhy*, June 5, 2020.
9. Gabriella Novello, “[Trump Doesn’t Let Pandemic Curb His War On Absentee Ballots](#),” *WhoWhatWhy*, May 26, 2020.
10. Gabriella Novello, “[Absentee Voting in New York Seen as a ‘Challenging and Scary’ Experience](#),” *WhoWhatWhy*, June 26, 2020.
11. “[State Election Law Overview](#),” Lawyers’ Committee for Civil Rights Under Law, April 27, 2020.
12. Gabriella Novello, “[Georgia Certifies Election Results Despite Serious](#)

- [Flaw in Ballot Scanners](#)," *WhoWhatWhy*, June 23, 2020.
13. Gabriella Novello, "[The Media's Most Important Job in 2020: Countering Postelection Chaos](#)," *WhoWhatWhy*, May 11, 2020.
  14. Gabriella Novello, "[America Decides, 2020: Voting by Mail, Explained](#)," *WhoWhatWhy*, July 30, 2020.
  15. Donald J. Trump, [Twitter Post](#), April 8, 2020, 7:34 PM.
  16. Stef W. Knight and Naema Ahmed, "[When and How to Vote in All 50 States](#)," *Axios*, August 13, 2020.

# ABOUT THE AUTHORS

---

## Celeste Katz Marston

Celeste's career spans 25 years of reporting for newspapers, magazines, and radio, with a special focus on voting rights and election administration. She has been on staff at the *New York Daily News*, *Newsweek*, WBAI Radio New York, Conde Nast, and the *Providence Journal*, among others, and has contributed freelance reporting to outlets including Hearst Magazines, SiriusXM, and the *Boston Globe*. She has covered five presidential elections and numerous races for the Senate and House, and has reported from New York City Hall and the State Capitol. Her investigative work has exposed government secrecy, nepotism, and questionable use of taxpayer and corporate dollars, leading to public policy changes and calls for federal and local investigations. Celeste holds a BA in international relations from Brown University.

## Gabriella Novello

Gabriella joined *WhoWhatWhy* in June 2019 as an election integrity fellow, reporting on the state of voting rights and election infrastructure in the United States. Some of Gabriella's reporting includes stories on Georgia residents' efforts to request a re-certification of the state's newly purchased voting system and cyber vulnerabilities that were discovered in various election equipment. She also reported on the North Carolina State Board of Elections' decision to approve new voting machines without undergoing a

certification process as required by state law. An alumnae of the American University in Washington, DC, she received her bachelor's in journalism with a minor in health promotion. In addition to her work with *WhoWhatWhy*, Gabriella also reports on the Colorado congressional delegation for the *Colorado Times Recorder*.

# ABOUT WHOWHATWHY

---

*WhoWhatWhy* is a nonprofit, nonpartisan news organization embodying a form of investigative reporting that is rigorous, relentless, and scientific — we call it forensic journalism.

Forensic journalism requires skepticism toward power and credentialed expertise; a determination to unearth the facts that interested parties want to keep hidden; and an unflinching commitment to follow the trail wherever it leads.

Please visit our website, where you can read our daily articles and sign up for our newsletters.

# GLOSSARY

---

## Americans with Disabilities Act (ADA)

*a civil rights law prohibiting discrimination against individuals with disabilities in all areas of public life, including jobs, schools, transportation, and all public and private places that are open to the general public — which means voting, as well. The purpose of the law is to make sure that people with disabilities have the same rights and opportunities as everyone else.*

## ballot-marking device (BMD)

*a ballot-marking device, or vote recorder, is a type of voting machine used by voters to record votes on physical ballots. In general, ballot-marking devices neither store nor tabulate ballots, but only allow the voter to record votes on ballots that are then stored and tabulated elsewhere.*

## DEF CON

*DEFCON is a large and well-known hacker conference. Its Voter Village is one of dozens of working groups which put on activities for participants. In the Voter Village, hackers are tasked with breaking into voting machines, and identifying vulnerabilities in US voting systems.*

### direct-recording electronic (DRE)

*voting machine that records votes by a ballot display with electro-optical components that can be activated by the voter. A direct-recording electronic device processes data by means of a computer program. It records voting data and ballot images in memory components. It then tabulates voting data stored in a removable memory card and sometimes as a printed copy.*

### Election Assistance Commission (EAC)

*an independent national clearinghouse and resource of information regarding election administration. It is charged with administering payments to states and developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, accrediting voting system test laboratories, and certifying voting equipment. It is also charged with developing and maintaining a national mail voter registration form.*

*The EAC creates and maintains the Voluntary Voting System Guidelines; creates a national program for the testing, certification, and decertification of voting systems; and maintains the National Mail Voter Registration Form required by the National Voter Registration Act of 1993. It reports to Congress every two years on the effects of the NVRA on elections; administers federal funds to states for HAVA requirements and for the development of innovative election technology, including pilot programs to test election technology; studies and reports best practices of effective administration; and communicates information on laws, technologies, procedures, studies, and data related to the administration of federal elections to those responsible for*

*formulating or implementing election law and procedures — as well as to the media, and to other interested persons.*

#### electronic poll book

*a system containing an electronic list of registered voters that may be transported to the polling location. It contains voter name, address, district or precinct, party preference, voter status, whether the voter was issued a mail-in ballot, whether that ballot has been recorded as accepted by an elections official, and whether or not that voter's ID must be verified.*

#### electronic voting

voting that uses electronic means to either aid or take care of casting and counting votes. May use standalone electronic voting machines and encompass a range of internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption, transmission to servers, and consolidation and tabulation of election results.

Electronic voting technology can include punch cards, optical scan voting systems, and specialized voting kiosks (including self-contained direct-recording electronic voting). It can also involve transmission of ballots and votes via telephones, private computer networks, or the internet.



### electronic voting machine

*a computer connected to the internet for ease of voting.*

### Help America Vote Act

*a US federal law which passed 357–48 in the House and 92–2 in the Senate and was signed into law by President George W. Bush on October 29, 2002. The bill was drafted (at least in part) in reaction to the controversy surrounding the 2000 election when almost two million ballots were disqualified because they registered multiple votes or none when run through vote-counting machines.*

*The goals of HAVA are to replace punch-card and lever-based voting systems, to create the Election Assistance Commission to assist in the administration of federal elections, and to establish minimum election admissions standards.*

### National Voter Registration Act

*advances voting rights in the United States by requiring state governments to offer voter registration opportunities to any eligible person who applies for or renews a driver's license or applies for public assistance along with requiring USPS to mail election materials. The law requires states to register applicants that use a federal voter registration form to apply and prohibits states from removing registered voters from the voter rolls unless certain criteria are met.*

### optical scanner

*electronic device that reads marked paper ballots and tallies the results.*

### Organization for Economic Cooperation and Development (OECD)

*an intergovernmental economic organization with 37 member countries, founded in 1961 to stimulate economic progress and world trade. It is a forum of countries describing themselves as committed to democracy and the market economy. It provides a platform to compare policy experiences, seek answers to common problems, identify good practices, and coordinate domestic and international policies of its members.*

### quick response code (QR code)

*a barcode first designed in 1994 for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. In practice, QR codes often contain data for a locator, identifier, or tracker that points to a website or application. They are being used in some voting machines to tabulate votes.*

### risk-limiting audit

*one way of checking whether computers tallied an election accurately. It involves storing paper ballots securely until they can be checked, and manually comparing a statistical sample of paper*

*ballots to the computer records for those same ballots, then checking whether all the computer records of ballots in the election were totalled correctly. If the small sample has a large enough margin, it can be used in place of a total manual recount.*

### Voluntary Voting System Guidelines

*federal guidelines providing background information about voting system standards; the purpose and scope; an overview of new and expanded material; and general core requirements for voting systems and voting devices. It includes security and audit architecture; usability, accessibility, and privacy requirements; security and general core requirements; contains requirements that apply to the technical data package, voting equipment user documentation, the test plan, the test report, the public information package, and data for repositories; and describes the way voting system test laboratories are to determine if voting systems, voting devices, and software meet the requirements of the VVSG.*

### voting machine

*a machine used to register and tabulate votes. Voting machines have different levels of usability, security, efficiency, and accuracy. Certain systems may be more or less accessible to all voters, or not accessible to those voters with certain types of disabilities. They can also have an effect on the public's ability to oversee elections.*