Businessweek

How US Voting Machines Became Safer Than Ever

Clear Ballot shows just how slow, steady and paper-dependent the industry is.

By Austin Carr
Photographs by Philip Montgomery for Bloomberg Businessweek
October 30, 2024 at 4:00 AM EDT, *Updated October 30, 2024 at 1:20 PM EDT*

Share this article

Chip Trowbridge is confident his voting machines are secure, but he'll run the thought experiment with you. An assortment of the machines are resting on a counter at the downtown Boston office of Clear Ballot Group Inc., and Trowbridge, the company's chief technology officer, is facetiously pointing out the bonkers number of steps a

bad actor would need to take to compromise one of its ClearCast computer scanners. Any tampering would have to take place on-site, because the ClearCast systems aren't connected to the internet. Most arrive at county voting precincts in fastened containers or locked cages. "There's one 120-volt plug out the back, and that's it—no Wi-Fi, no Bluetooth, no Ethernet, no nothing," Trowbridge says. Republican and Democratic officials are supposed to set them up together by tearing security seals with identifying serial numbers and entering unique passwords after booting them up. Data is stored on three redundant drives, including two locked-in USB sticks, and any poll worker inputs on the devices (such as removing one of the sticks) are logged by the equivalent of an airplane's black box.

Then there's the paper trail. On Election Day, voters feed their handmarked ballots into the scanner, which is the size of a cash register and has a thick screen on top. It tabulates blackened ovals and captures a digital image of the entire slip for backup, then spits the ballot down into a bolted cabinet so it can be audited by hand if needed. The scanners are tested with sample votes beforehand, and often afterward, to ensure there are no discrepancies between digital counts and physical entries.

Each Clear Ballot voting machine logs all the actions it takes. At the end of each day, election officials can print a summary of that activity—everything from how many votes it recorded to how often it suffered a paper jam.

An employee checks the headphones that talk visually impaired people through casting their votes. Increased accessibility has been a leading driver of the modest technological updates to US voting machines of late.

As Trowbridge entertains and ultimately shoots down increasingly absurd but-what-about-this scenarios, such as <u>counterfeit ballots</u> or <u>malware-laced thumb drives</u>, he stops short with a frank reminder: "We're already in crazy territory if any of this is happening."

Clear Ballot and its larger rivals, Dominion Voting Systems Corp. and Election Systems & Software LLC, operate in a different kind of

crazy territory these days. The industry has long experienced perpetual upheaval. Following the paper-ballot fiasco of 2000 (hanging chads, anyone?), sweeping regulations pushed the US from punch cards to paperless DREs, or direct-recording electronics. Voters hit buttons or a touchscreen, and their selections were programmed into the computer's memory. But DREs fell out of favor in the 2010s, because the virtual approach didn't allow for manual recounts, and they were hard to check for inaccuracies and meddling. So began a shift back to physical ballots, particularly after Hillary Clinton lost to Donald Trump and Democrats howled about Russian interference and questioned the 2016 election's legitimacy.

Now, the voting system industry is besieged by conspiracy theories, including from the likes of Elon Musk, about mass hacking and rigging of electronic voting machines. And yet the technology is extremely conservative–even tech from relative newcomers such as Clear Ballot, whose products have been certified for use in 14 states, including Pennsylvania, Ohio and Wisconsin. The paranoia, combined with the usual pace of government bureaucracy, is keeping anyone from pushing boundaries.
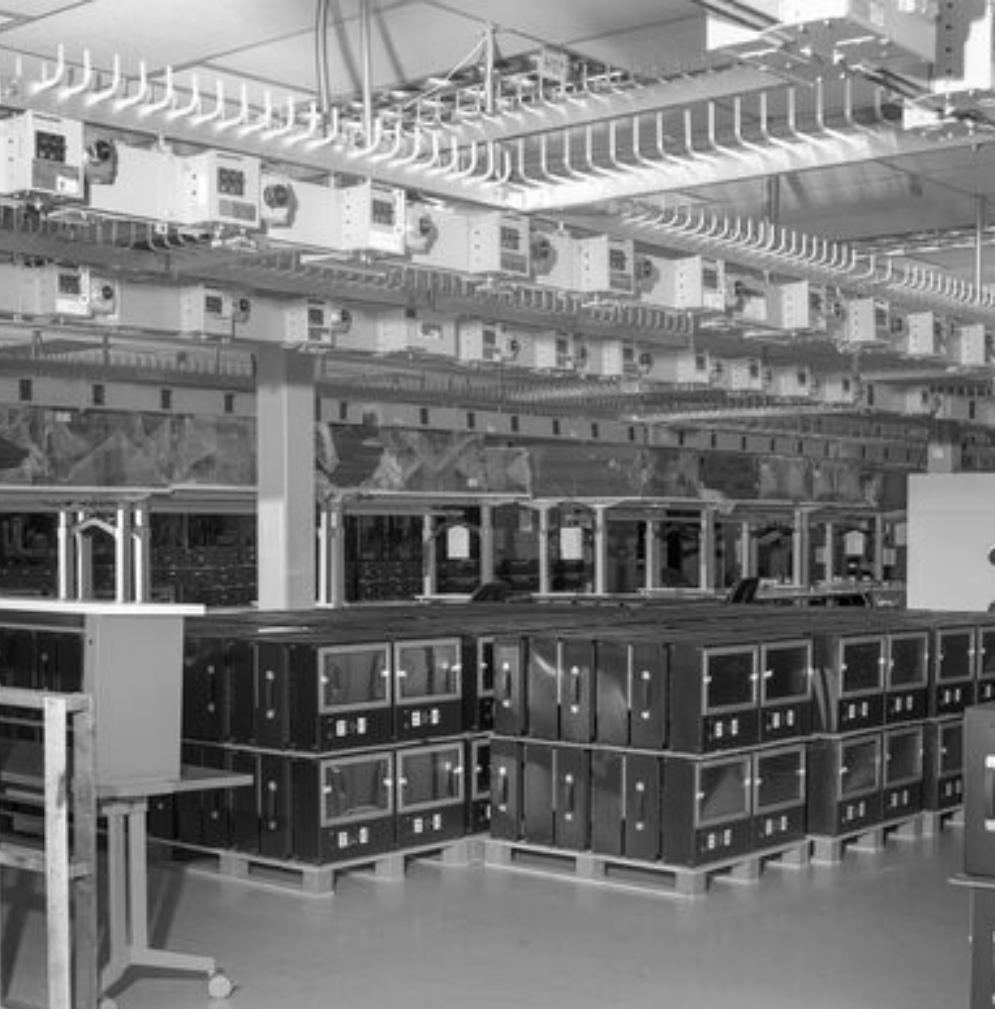
Machines at Clear Ballot's manufacturing facility in New Hampshire. To help guard against tampering and protect employee safety, the company insists on keeping the facility's precise location a secret.

Voting machines
undergoing final
inspections before
they're shipped to
counties across the US.

Clear Ballot got its start more than a decade ago, building software to automate inspections of Dominion and ES&S ballots. Its founders and engineers were veterans of Endeca Technologies Inc., which developed e-commerce infrastructure and data analytics for retailers such as Target and Walmart. (Oracle Corp. acquired Endeca in 2011 for $1.1 billion.) Clear Ballot's main differentiator was a tool that catalogs the ovals voters fill in at the polls and lets election officials visualize them on a screen for auditing purposes.

Some voters are lousy at filling out ballots. They may shade only part of the bubble next to the name of their preferred candidate or scribble sloppily in and out of the borders. They may check off their choices, inadvertently dot multiple options as they

deliberate, or X out a mistaken entry and circle a different one. Clear Ballot's software captures the inky mess and lets officials scour it in a simple app interface.
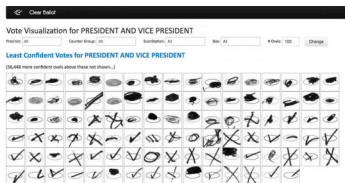
Clear Ballot's visualization software helps election officials review ballots with messy oval markings. *Courtesy of Clear Ballot*

On the app, the marked ovals for each race and ballot initiative are arranged in a grid, like a police index of fingerprints, in order of confidence level. The vast majority of ovals tend to be properly filled and are easy for the scanner to read. The app then separates those ovals from the weirder batches that need human review. The hope is that

this routine will lead to faster adjudications in the event of a tight finish, because the trailing candidate can quickly see if there are anywhere near close to enough contestable entries to justify a recount. "It ranks and sorts those ovals and brings the needles in the haystack right to the forefront for human eyes," says elections supervisor Mark Earley of Leon County, Florida, one of the first places to embrace Clear Ballot's tech. "When folks from the election world–candidates, attorneys, legislators–see this visualization tool, their jaws just hang open, like, Oh my God, this is so powerful." (Today, 80% of the Sunshine State, by share of registered voters, uses it for audits.)

The ClearCast scanner digitizes ballots and captures backup images of each vote for safekeeping. It's shipped in the same kind of crate used to transport gear for the likes of Aerosmith and U2.
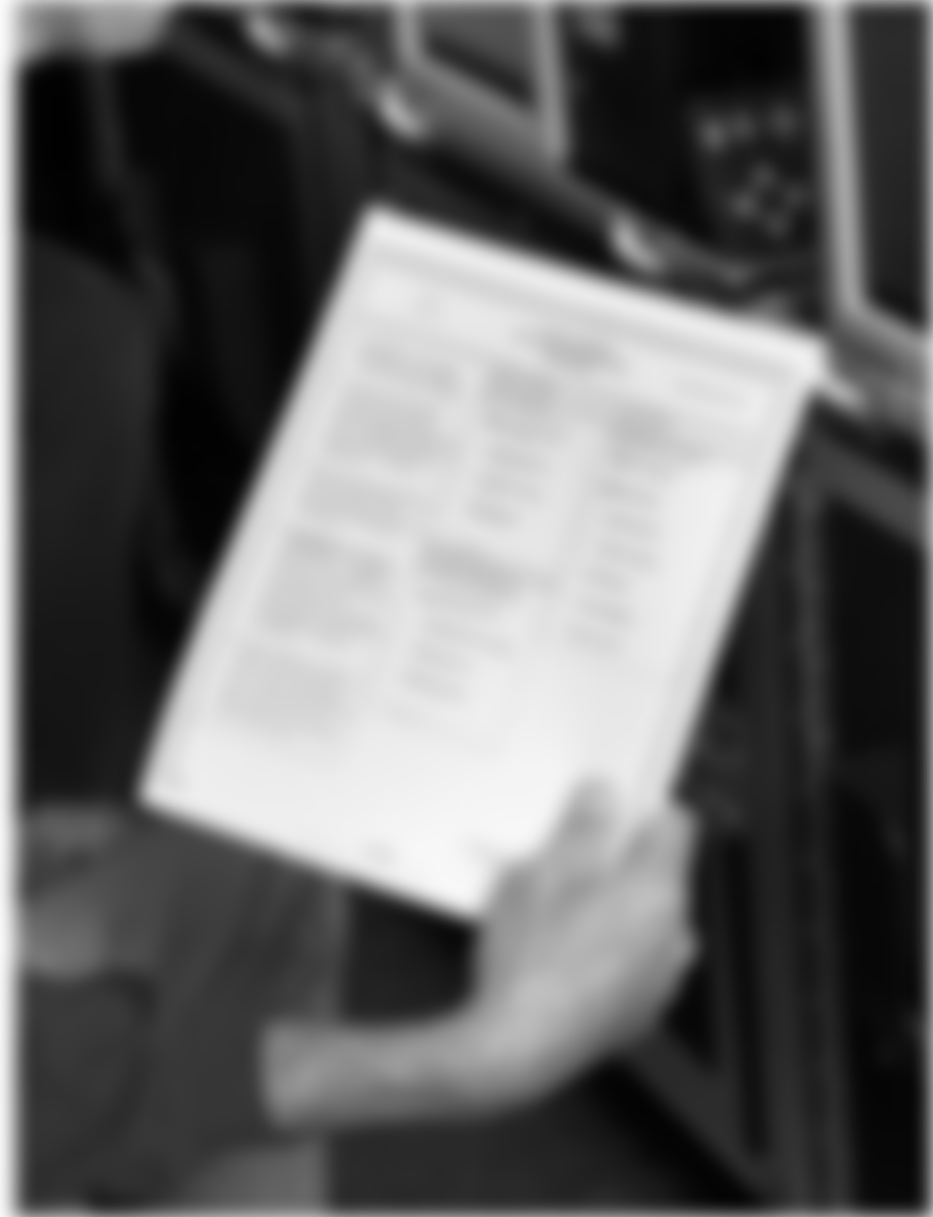
Clear Ballot's system is fundamentally paper-based. Each vote is marked by hand before being backed up digitally for speedier reporting.

The service caught on in Vermont, too, then in Maryland. By 2016 the company's annual revenue had reached seven figures. It soon raised $18 million from Bessemer Venture Partners and other investors after deciding to take on the incumbents with its own voting equipment, first in Oregon with a vote-by-mail system. While not exactly un-clunky, Clear Ballot's machines were a big step up from the hardware of the day. The competition "looked like old PCs you'd see at the dump," says Chief Executive Officer Bob Hoyt, who has the

ruddy mug and accent of a Beanpot hockey coach.

Clear Ballot's first in-person voting system was really just an extension of its paper-based audits, with computer programs and other gear for managing the election process from start to finish. After receiving federal certification in 2018, it was adopted in parts of Ohio and Wisconsin. Administrators appreciated the real-time digital count of submitted votes displayed on each ClearCast screen, which let them confirm that the total equaled the number of voters who'd entered the poll site. "If you have 100,000 ballots, but only 90,000 people came through the door–boom, somebody put 10,000 ballots through these machines," Hoyt says.

Even as Clear Ballot added more digital and analog safeguards to its products, Hoyt noticed the "tinfoil-hat people" growing louder. He recalls a competitor leaning into fears of bias and implying Clear Ballot's software couldn't be trusted, because it was coded in deep-blue Massachusetts. "I was called a bleeding liberal Obama fanatic," Hoyt remembers, chuckling. "I was like, Jesus Christ, I'm from New Hampshire!"
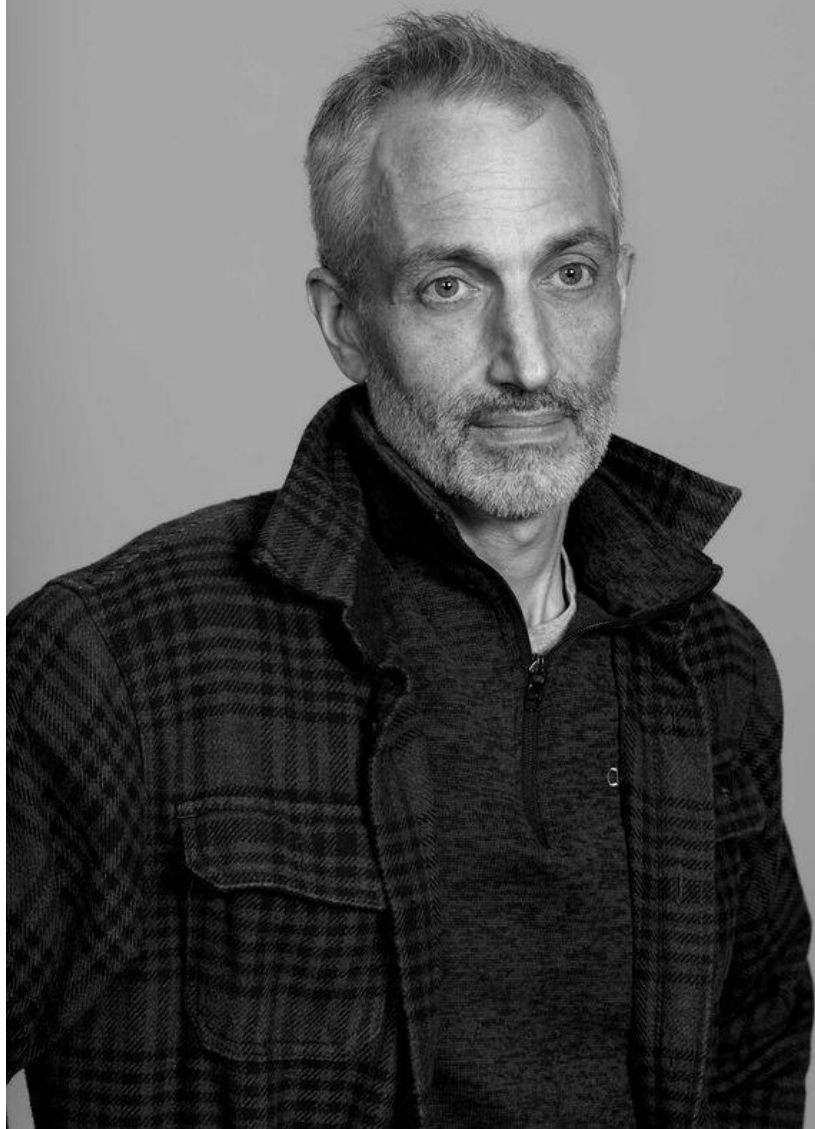
Trowbridge believes disinformation amplified by Elon Musk and other conspiratorial voices is a greater threat to elections than the potential hacking of voting machines.

After the 2020 election, Trump and other Republicans, hollering about rigged Dominion machines, attempted to overturn Joe Biden's victory. Trump allies claimed, without any actual evidence, that Biden had effectively stolen the election by using foreign servers to transmit fake votes, among other conspiracy theories. In 2021, Clear Ballot offered to audit the high-profile election challenges still taking place in Arizona's Maricopa County for $450,000, but it never heard back from the state's Republican-controlled Senate. Instead, Arizona hired

Cyber Ninjas Inc., an obscure firm with ties to Trump's "Stop the Steal" movement but no audit experience. Cyber Ninjas released a now-discredited report and has since gone out of business. One accounting analysis found that the bogus endeavor cost Arizona taxpayers around $3 million. (Fox News, which amplified questionable claims about Dominion machines, later agreed to pay the company $787 million to settle a defamation lawsuit.)

Clear Ballot had its own 2020 election headache to deal with in Pennsylvania's rural Lycoming County, where GOP rabble-rousers accused it of illegally switching troves of votes, for reasons unclear. (Trump won the district.) They eventually forced the county to perform a labor-intensive hand recount last year, well into Biden's presidency. In the end,

Trump gained a measly eight votes out of the 59,397 cast, a discrepancy Lycoming's elections director, Forrest Lehman, chalks up to minor differences in interpreting a small number of oval markings.

ClearCast scanners do occasionally encounter confusing smudges. In 2020 hand sanitizers caused stains on some mail-in ballots. Humans reviewing digitally flagged ovals can misjudge the voter's intent. But these issues usually represent a rounding error, and the digital review brings more transparency and recordkeeping to a common part of the election resolution process. "Folks think every election should be perfect," Lehman says. "And if it's not, the first explanation is that something fraudulent must've happened, like, you know, 'The Hamburglar came through the window.'"

Clear Ballot voting machines have been certified in 14 US states.

Mobility is key. Black trunk cases with strengthened rolling wheels allow poll workers to more easily slide the voting machines up ramps and over doorway bumps at school gyms and other poll sites.

ON A LATE SEPTEMBER MORNING AT CLEAR Ballot's New Hampshire manufacturing facility, Trowbridge is excited to show off a recent upgrade: better wheels. Dozens of shiny new ClearCasts are awaiting shipment in black trunk cases, similar to the ones rock bands use to transport instruments. He's pumped about the wheels underneath. The company replaced the stock wheels with stronger ones and kick brakes, so workers can more easily slide the equipment up ramps and over doorway bumps at school gyms and other poll sites. The tweak required complicated engineering approvals with the US Election Assistance Commission, the federal agency that oversees voting systems. "It took five months," Trowbridge says.

Approvals for custom electronics inevitably take longer. The EAC's certification process is absurdly rigorous and slow, based on more than 1,000 requirements. There are only two independent labs, in Alabama and Colorado, that handle the EAC's compliance testing, and their backlogs are insane. (Neither lab responded to requests for comment.) Evaluations for brand-new systems complying with the EAC's latest standards are expected to take as long as 18 months; even testing for merely modified systems averages around seven months. This helps explain why voting machines aren't what you'd call sleek. "They certainly don't look like an Apple device," Trowbridge acknowledges wryly.

There's a vague perception that election computers are complex when, in reality, they generally consist of basic proprietary hardware mixed with off-the-shelf components from the likes of Dell and SanDisk. Clear Ballot depends on Fujitsu scanners for bigger tabulation jobs. Clear Ballot has to stockpile enough parts for future sales of its machines rather than betting that suppliers will keep making them. An unexpected change to one of the components could mean months of paperwork to integrate its replacement, though the EAC says approvals for more minor tweaks are much faster.
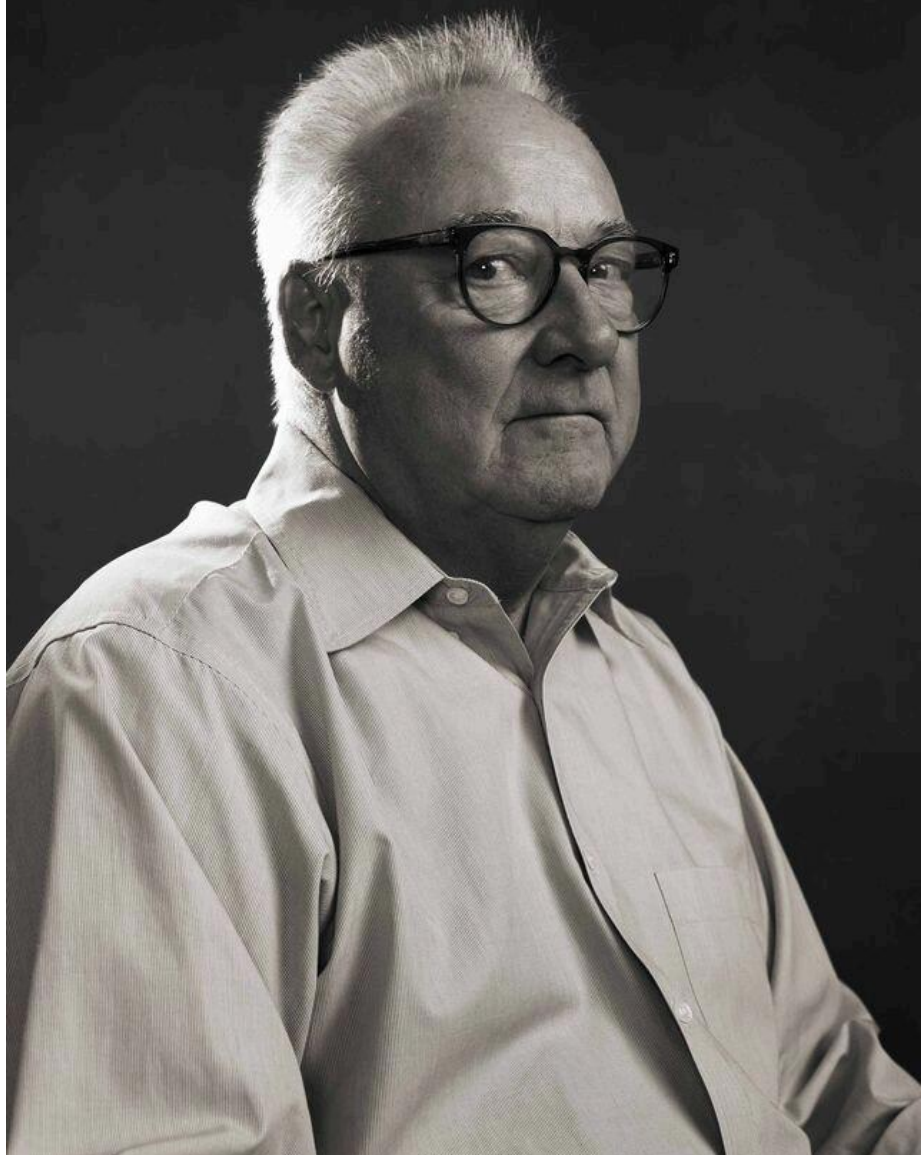
Relying on dated and generic components may not sound secure, but it guarantees the systems aren't driven by untested advances in, say, artificial intelligence. There are only six current EAC-approved makers of voting machines, and they mostly distinguish themselves with customer service, software interfaces, pricing and hardware ergonomics like improved wheels.

In keeping with the trend toward stripping away tech, the EAC's latest guidelines banned cellular modems, which older machines historically used to transmit unofficial results from precincts to centralized county offices on election night. Some cybersecurity experts also want to do away with air-gapped local networks, which can't connect to the internet but do allow computers at the same voting place to communicate with one another.

Such pressures are already disrupting some of the industry's flagship offerings. In Georgia, for example, Dominion's ImageCast X lets voters tap choices on a touchscreen, then prints their selections on a summary receipt in plain text with a corresponding QR code. Voters deposit the receipt into a separate Dominion tabulator, which scans the code

and tallies the vote. But anxieties over whether the QR data matches what people actually selected have led to a huge push to revert to pens and Sharpies. (A published advisory from the US Cybersecurity and Infrastructure Security Agency said there's <u>no evidence</u> any vulnerabilities of this Dominion system have ever been exploited in an election. Dominion has said its machines have many layers of physical and operational safeguards.)

As much as Trowbridge and Hoyt slag their rivals, they're confident the competing products work fine, in part because the EAC mandates that they function in similar,

intentionally limited ways. "Voting machines are stupid!" Hoyt says. "You put a ballot in, and it reads the ballot. If you have to do a hand recount, you have the paper backup." Of course, that's not to imply that machines, or really any electronic voting systems, are infallible. A 2019 University of Michigan research paper found that injecting malware composed of just 398 lines of code into a Clear Ballot scanner could trick it into altering ballot images, so a written "Yes" vote would transfer digitally as a "No" vote on the connected computer. However, it was more a test of whether tampering was theoretically possible rather than practically feasible at scale. Clear Ballot says that the research paper didn't adequately account for myriad safeguards that would make such an attack virtually impossible, including pre- and post-

election accuracy testing, separate audits and recounts, and physical security and machine protocols that would identify rogue behavior. Pulling it off in the real world wouldn't merely require *Mission: Impossible*-level cunning; it would take the logistical omnipresence of Santa Claus. You'd need unfettered in-person access to a Clear Ballot system, then you'd have to crack open its sealed encasing without raising red flags with precinct authorities. You'd need to somehow stop auditors and central county offices from ever checking or retabulating the corresponding paper ballots–a random sample of which are reviewed by hand to avoid anomalies with electronic results. And then, congratulations, you've broken into one machine. "There's probably a thousand alone in the city of

Cleveland," Hoyt says. Good luck hacking the rest.

Nevertheless, the imagined vulnerabilities have fueled calls for a complete move to analog processes. "We should eliminate electronic voting machines. The risk of being hacked by humans or AI, while small, is still too high," Musk posted on X earlier this year. Trump has lately been pushing for all ballots to be hand-counted when polls close on Nov. 5 in his battle with Kamala Harris.

"Elon should know better," says Trowbridge, noting that hand counts are ripe for the potential (and perception) of human error and malfeasance. They're also slow. At the

rate it took tiny Lycoming County to complete its manual recount, it would take 100,000 full-time workers at least two to three weeks to comb through the 160 million votes expected to be cast in the 2024 presidential election. And that's assuming perfect speed and accuracy, no clerical disputes or interruptions and ballots with only 10 contests. (This figure can be much higher depending on the area; Maricopa County will average 79 contests per ballot this year.) Partisan fighting over hand counts was partly why the US shifted to faster, systematized computers to improve the process. "There's a reason that nobody hand-grades the SATs," says EAC Chairman Ben Hovland. "We can have equipment do this in a more accurate and efficient way."

The Clear Ballot team says much greater election threats stem from disinformation, voter-registration manipulation and malicious targeting of poll-site staffers. Trowbridge says he always hears from these workers that they just want basic tools to do their jobs better and faster, so they can stay out of the news and ideally get to bed before midnight. They're tired of all the distractions.

(Corrects second paragraph to amend plug voltage. An earlier version of this story updated the 10th paragraph to add investor details and corrected the identification of the person in the second inline photo caption.)

More On Bloomberg