The New York Times
nytimes.com

January 6, 2008

Can You Count on Voting Machines?

By CLIVE THOMPSON

Jane Platten gestured, bleary-eyed, into the secure room filled with voting machines. It was 3 a.m. on Nov. 7, and she had been working for 22 hours straight. “I guess we’ve seen how technology can affect an election,” she said. The electronic voting machines in Cleveland were causing trouble again.

For a while, it had looked as if things would go smoothly for the Board of Elections office in Cuyahoga County, Ohio. About 200,000 voters had trooped out on the first Tuesday in November for the lightly attended local elections, tapping their choices onto the county’s 5,729 touch-screen voting machines. The elections staff had collected electronic copies of the votes on memory cards and taken them to the main office, where dozens of workers inside a secure, glass-encased room fed them into the “GEMS server,” a gleaming silver Dell desktop computer that tallies the votes.

Then at 10 p.m., the server suddenly froze up and stopped counting votes. Cuyahoga County technicians clustered around the computer, debating what to do. A young, business-suited employee from Diebold — the company that makes the voting machines used in Cuyahoga — peered into the screen and pecked at the keyboard. No one could figure out what was wrong. So, like anyone faced with a misbehaving computer, they simply turned it off and on again. Voilà: It started working — until an hour later, when it crashed a second time. Again, they rebooted. By the wee hours, the server mystery still hadn’t been solved.

Worse was yet to come. When the votes were finally tallied the next day, 10 races were so close that they needed to be recounted. But when Platten went to retrieve paper copies of each vote — generated by the Diebold machines as they worked — she discovered that so many printers had jammed that 20 percent of the machines involved in the recounted races lacked paper copies of some of the votes. They weren’t lost, technically speaking; Platten could hit “print” and a machine would generate a replacement copy. But she had no way of proving that these replacements were, indeed, what the voters had voted. She could only hope the machines had worked correctly.

As the primaries start in New Hampshire this week and roll on through the next few months, the erratic behavior of voting technology will once again find itself under a microscope. In the last three election cycles, touch-screen machines have become one of the most mysterious and divisive elements in modern electoral politics. Introduced after the 2000 hanging-chad debacle, the machines were originally intended to add clarity to election results. But in hundreds of instances, the result has been precisely the opposite: they fail unpredictably, and in extremely strange ways; voters report that their choices “flip” from one candidate to another before their eyes; machines crash or begin to count backward; votes simply vanish. (In the 80-person town of Waldenburg, Ark., touch-screen machines tallied zero votes for one mayoral candidate in 2006 — even though he’s pretty sure he voted for himself.) Most famously, in the November 2006 Congressional election in Sarasota, Fla., touch-screen machines recorded an 18,000-person “undervote” for a race decided by fewer than 400 votes.

The earliest critiques of digital voting booths came from the fringe — disgruntled citizens and scared-senseless computer geeks — but the fears have now risen to the highest levels of government. One by one, states are renouncing the use of

touch-screen voting machines. California and Florida decided to get rid of their electronic voting machines last spring, and last month, Colorado decertified about half of its touch-screen devices. Also last month, Jennifer Brunner, the Ohio secretary of state, released a report in the wake of the Cuyahoga crashes arguing that touch-screens "may jeopardize the integrity of the voting process." She was so worried she is now forcing Cuyahoga to scrap its touch-screen machines and go back to paper-based voting — before the Ohio primary, scheduled for March 4. Senator Bill Nelson, a Democrat of Florida, and Senator Sheldon Whitehouse, Democrat of Rhode Island, have even sponsored a bill that would ban the use of touch-screen machines across the country by 2012.

It's difficult to say how often votes have genuinely gone astray. Michael Shamos, a computer scientist at Carnegie Mellon University who has examined voting-machine systems for more than 25 years, estimates that about 10 percent of the touch-screen machines "fail" in each election. "In general, those failures result in the loss of zero or one vote," he told me. "But they're very disturbing to the public."

Indeed, in a more sanguine political environment, this level of error might be considered acceptable. But in today's highly partisan and divided country, elections can be decided by unusually slim margins — and are often bitterly contested. The mistrust of touch-screen machines is thus equal parts technological and ideological. "A tiny number of votes can have a huge impact, so machines are part of the era of sweaty palms," says Doug Chapin, the director of Electionline.org, a nonpartisan group that monitors voting reform. Critics have spent years fretting over corruption and the specter of partisan hackers throwing an election. But the real problem may simply be inherent in the nature of computers: they can be precise but also capricious, prone to malfunctions we simply can't anticipate.

During this year's presidential primaries, roughly one-third of all votes will be cast on touch-screen machines. (New Hampshire voters are not in this group; they will vote on paper ballots, some of which are counted in optical scanners.) The same ratio is expected to hold when Americans choose their president in the fall. It is a very large chunk of the electorate. So what scares election observers is this: What happens if the next presidential election is extremely close and decided by a handful of votes cast on machines that crashed? Will voters accept a presidency decided by ballots that weren't backed up on paper and existed only on a computer drive? And what if they don't?

"The issue for me is the unknown," Platten told me when we first spoke on the phone, back in October. "There's always the unknown factor. Something — something — happens every election."

NEW VOTING TECHNOLOGIES tend to emerge out of crises of confidence. We change systems only rarely and in response to a public anxiety that electoral results can no longer be trusted. America voted on paper in the 19th century, until ballot-box stuffing — and inept poll workers who lost bags of votes — led many to abandon that system. Some elections officials next adopted lever machines, which record each vote mechanically. But lever machines have problems of their own, not least that they make meaningful recounts impossible because they do not preserve each individual vote. Beginning in the 1960s they were widely replaced by punch-card systems, in which voters knock holes in ballots, and the ballots can be stored for a recount. Punch cards worked for decades without controversy.

Until, of course, the electoral fiasco of 2000. During the Florida recount in the Bush-Gore election, it became clear that punch cards had a potentially tragic flaw: "hanging chads." Thousands of voters failed to punch a hole clean through the ballot, turning the recount into a torturous argument over "voter intent." On top of that, many voters confused by the infamous "butterfly ballot" seem to have mistakenly picked the wrong candidate. Given Bush's microscopic margin of victory — he was ahead by only a few hundred votes statewide — the chads produced the brutal, monthlong legal brawl over how and whether the recounts should be conducted.

The 2000 election illustrated the cardinal rule of voting systems: if they produce ambiguous results, they are doomed to suspicion. The election is never settled in the mind of the public. To this date, many Gore supporters refuse to accept the legitimacy of George W. Bush's presidency; and by ultimately deciding the 2000 presidential election, the Supreme Court was pilloried for appearing overly partisan.

Many worried that another similar trauma would do irreparable harm to the electoral system. So in 2002, Congress passed the Help America Vote Act (HAVA), which gave incentives to replace punch-card machines and lever machines and authorized $3.9 billion for states to buy new technology, among other things. At the time, the four main vendors of voting machines — Diebold, ES&S, Sequoia and Hart — were aggressively marketing their new touch-screen machines. Computers seemed like the perfect answer to the hanging chad. Touch-screen machines would be clear and legible, unlike the nightmarishly unreadable "butterfly ballot." The results could be tabulated very quickly after the polls closed. And best of all, the vote totals would be conclusive, since the votes would be stored in crisp digital memory. (Touch-screen machines were also promoted as a way to allow the blind or paralyzed to vote, via audio prompts and puff tubes. This became a powerful incentive, because, at the behest of groups representing the disabled, HAVA required each poll station to have at least one "accessible" machine.)

HAVA offered no assistance or guidelines as to what type of machine to buy, and local elections officials did not have many resources to investigate the choices; indeed, theirs are some of most neglected and understaffed offices around, because who pays attention to electoral technology between campaigns? As touch-screen vendors lobbied elections boards, the machines took on an air of inevitability. For elections directors terrified of presiding over "the next Florida," the cool digital precision of touch-screens seemed like the perfect antidote.

IN THE LOBBY OF JANE PLATTEN'S OFFICE in Cleveland sits an AccuVote-TSX, made by Diebold. It is the machine that Cuyahoga County votes on, and it works like this: Inside each machine there is a computer roughly as powerful and flexible as a modern hand-held organizer. It runs Windows CE as its operating system, and Diebold has installed its own specialized voting software to run on top of Windows. When the voters tap the screen to indicate their choices, the computer records each choice on a flash-memory card that fits in a slot on the machine, much as a flash card stores pictures on your digital camera. At the end of the election night, these cards are taken to the county's election headquarters and tallied by the GEMS server. In case a memory card is accidentally lost or destroyed, the computer also stores each vote on a different chip inside the machine; election officials can open the voting machine and remove the chip in an emergency.

But there is also a third place the vote is recorded. Next to each machine's LCD screen, there is a printer much like one on a cash register. Each time a voter picks a candidate on screen, the printer types up the selections, in small, eight-point letters. Before the voter pushes "vote," she's supposed to peer down at the ribbon of paper — which sits beneath a layer of see-through plastic, to prevent tampering — and verify that the machine has, in fact, correctly recorded her choices. (She can't take the paper vote with her as proof; the spool of paper remains locked inside the machine until the end of the day.)

Under Ohio law, the paper copy *is* the voter's vote. The digital version is not. That's because the voter can see the paper vote and verify that it's correct, which she cannot do with the digital one. The digital records are, in essence, merely handy additional copies that allow the county to rapidly tally potentially a million votes in a single evening, whereas counting the paper ballots would take weeks. Theoretically speaking, the machine offers the best of all possible worlds. By using both paper and digital copies, the AccuVote promised Cuyahoga an election that would be speedy, reliable and relatively inexpensive.

Little of this held true. When the machines were first used in Cuyahoga Country during the May 2006 primaries, costs ballooned — and chaos reigned. The poll workers, many senior citizens who had spent decades setting up low-tech punch-card systems, were baffled by the new computerized system and the rather poorly written manuals from Diebold and the county. “It was insane,” one former poll worker told me. “A lot of people over the age of 60, trying to figure out these machines.” Since the votes were ferried to the head office on small, pocket-size memory cards, it was easy for them to be misplaced, and dozens went missing.

On Election Day, poll workers complained that 143 machines were broken; dozens of other machines had printer jams or mysteriously powered down. More than 200 voter-card encoders — which create the cards that let voters vote — went missing. When the machines weren’t malfunctioning, they produced errors at a stunning rate: one audit of the election discovered that in 72.5 percent of the audited machines, the paper trail did not match the digital tally on the memory cards.

This was hardly the first such incident involving touch-screen machines. So it came as little surprise that Diebold, a company once known primarily for making safes and A.T.M.’s, subsequently tried to sell off its voting-machine business and, failing to find a buyer, last August changed the name of the division to Premier Election Solutions (an analyst told American Banker that the voting machines were responsible for “5 percent of revenue and 100 percent of bad public relations”).

Nearly a year after the May 2006 electoral disaster, Ohio’s new secretary of state, Jennifer Brunner, asked the entire four-person Cuyahoga elections board to resign, and Platten — then the interim director of the board — was tapped to clean up the mess. Platten had already instituted a blizzard of tiny fixes. She added responsibilities to the position of “Election Day technician” — filled by young, computer-savvy volunteers who could help the white-haired poll workers reboot touch-screens when they crashed. She bought plastic business-card binders to hold memory cards from a precinct, so none would be misplaced. “Robocalls” at home from a phone-calling service reminded volunteers to show up. Her staff rewrote the inscrutable Diebold manuals in plain English.

The results were immediate. Over the next several months, Cuyahoga’s elections ran with many fewer crashes and shorter lines of voters. Platten’s candor and hard work won her fans among even the most fanatical anti-touch-screen activists. “It’s a miracle,” I was told by Adele Eisner, a Cuyahoga County resident who has been a vocal critic of touch-screen machines. “Jane Platten actually understands that elections are for the people.” The previous board, Eisner went on to say, ridiculed critics who claimed the machines would be trouble and refused to meet with them; the new replacements, in contrast, sometimes seemed as skeptical about the voting machines as the activists, and Eisner was invited in to wander about on election night, videotaping the activity.

Still, the events of Election Day 2007 showed just how ingrained the problems with the touch-screens were. The printed paper trails caused serious headaches all day long: at one polling place, printers on most of the machines weren’t functioning the night before the polls opened. Fortunately, one of the Election Day technicians was James Diener, a gray-haired former computer-and-mechanical engineer who opened up the printers, discovered that metal parts were bent out of shape and managed to repair them. The problem, he declared cheerfully, was that the printers were simply “cheap quality” (a complaint I heard from many election critics). “I’m an old computer nerd,” Diener said. “I can do anything with computers. Nothing’s wrong with computers. But this is the worst way to run an election.”

He also pointed out several other problems with the machines, including the fact that the majority of voters he observed did not check the paper trail to see whether their votes were recorded correctly — even though that paper record is their legal ballot. (I noticed this myself, and many other poll workers told me the same thing.) Possibly they’re simply lazy, or the poll

workers forget to tell them to; or perhaps they're older and couldn't see the printer's tiny type anyway. And even if voters do check the paper trail, Diener pointed out, how do they know the machine is recording it for sure? "The whole printing thing is a farce," he said.

What's more, the poll workers regularly made security errors. When a touch-screen machine is turned on for the first time on Election Day, two observers from different parties are supposed to print and view the "zero tape" that shows there are no votes already recorded on the machine; a hacker could fix the vote by programming the machine to start, for example, with a negative total of votes for a candidate. Yet when I visited one Cleveland polling station at daybreak, the two checkers signed zero tapes without actually checking the zero totals. And then, of course, there were the server crashes, and the recording errors on 20 percent of the paper recount ballots.

Chris Riggall, a spokesman for Diebold, said that machine flaws were not necessarily to blame for the problems. The paper rolls were probably installed incorrectly by the poll workers. And in any case, he added, the paper trail was originally designed merely to help in auditing the accuracy of an election — it wasn't supposed to be robust enough to serve as a legal ballot, as Ohio chose to designate it. But the servers were indeed an issue of the machine's design; when his firm tested them weeks later, it found a data bottleneck that would need to be fixed with a software update.

The Nov. 6 vote in Cuyahoga County offered a sobering lesson. Having watched Platten's staff and the elections board in action, I could see they were a model of professionalism. Yet they still couldn't get their high-tech system to work as intended. For all their diligence and hard work, they were forced, in the end, to discard much of their paper and simply trust that the machines had recorded the votes accurately in digital memory.

THE QUESTION, OF COURSE, is whether the machines should be trusted to record votes accurately. Ed Felten doesn't think so. Felten is a computer scientist at Princeton University, and he has become famous for analyzing — and criticizing — touch-screen machines. In fact, the first serious critics of the machines — beginning 10 years ago — were computer scientists. One might expect computer scientists to be fans of computer-based vote-counting devices, but it turns out that the more you know about computers, the more likely you are to be terrified that they're running elections.

This is because computer scientists understand, from hard experience, that complex software can't function perfectly all the time. It's the nature of the beast. Myriad things can go wrong. The software might have bugs — errors in the code made by tired or overworked programmers. Or voters could do something the machines don't expect, like touching the screen in two places at once. "Computers crash and we don't know why," Felten told me. "That's just a routine part of computers."

One famous example is the "sliding finger bug" on the Diebold AccuVote-TSX, the machine used in Cuyahoga. In 2005, the state of California complained that the machines were crashing. In tests, Diebold determined that when voters tapped the final "cast vote" button, the machine would crash every few hundred ballots. They finally intuited the problem: their voting software runs on top of Windows CE, and if a voter accidentally dragged his finger downward while touching "cast vote" on the screen, Windows CE interpreted this as a "drag and drop" command. The programmers hadn't anticipated that Windows CE would do this, so they hadn't programmed a way for the machine to cope with it. The machine just crashed.

Even extremely careful programmers can accidentally create bugs like this. But critics also worry that touch-screen voting machines aren't designed very carefully at all. In the infrequent situations where computer scientists have gained access to the guts of a voting machine, they've found alarming design flaws. In 2003, Diebold employees accidentally posted the AccuVote's source code on the Internet; scientists who analyzed it found that, among other things, a hacker could program a voter card to let him cast as many votes as he liked. Ed Felten's lab, while analyzing an anonymously donated AccuVote-TS (a different model from the one used in Cuyahoga County) in 2006, discovered that the machine did not

“authenticate” software: it will run any code a hacker might surreptitiously install on an easily insertable flash-memory card. After California’s secretary of state hired computer scientists to review the state’s machines last spring, they found that on one vote-tallying server, the default password was set to the name of the vendor — something laughably easy for a hacker to guess.

But the truth is that it’s hard for computer scientists to figure out just how well or poorly the machines are made, because the vendors who make them keep the details of their manufacture tightly held. Like most software firms, they regard their “source code” — the computer programs that run on their machines — as a trade secret. The public is not allowed to see the code, so computer experts who wish to assess it for flaws and reliability can’t get access to it. Felten and voter rights groups argue that this “black box” culture of secrecy is the biggest single problem with voting machines. Because the machines are not transparent, their reliability cannot be trusted.

The touch-screen vendors disagree. They point out that a small number of approved elections officials in each state and county are allowed to hold a copy in escrow and to examine it (though they are required to sign nondisclosure agreements preventing them from discussing the software publicly). Further, vendors argue, the machines are almost always tested by the government before they’re permitted to be used. The Election Assistance Commission, a federal agency, this year began to fully certify four private-sector labs to stress-test machines. They subject them to environmental pressures like heat and vibration to ensure they won’t break down on Election Day; and they run mock elections, to verify that the machines can count correctly. In almost all cases, if a vendor updates the software or hardware, it must be tested all over again, which can take months. “It’s an extremely rigorous process,” says Ken Fields, a spokesman for the voting-machine company ES&S.

If the machines are tested and officials are able to examine the source code, you might wonder why machines with so many flaws and bugs have gotten through. It is, critics insist, because the testing is nowhere near dilligent enough, and the federal regulators are too sympathetic and cozy with the vendors. The 2002 federal guidelines, the latest under which machines currently in use were qualified, were vague about how much security testing the labs ought to do. The labs were also not required to test any machine’s underlying operating system, like Windows, for weaknesses.

Vendors paid for the tests themselves, and the results were considered proprietary, so the public couldn’t find out how they were conducted. The nation’s largest tester of voting machines, Ciber Inc., was temporarily suspended after federal officials found that the company could not properly document the tests it claimed to have performed.

“The types of malfunctions we’re seeing would be caught in a first-year computer science course,” says Lillie Coney, an associate director with the Electronic Privacy Information Commission, which is releasing a study later this month critical of the federal tests.

In any case, the federal testing is not, strictly speaking, mandatory. The vast majority of states “certify” their machines as roadworthy. But since testing is extremely expensive, many states, particularly smaller ones, simply accept whatever passes through a federal lab. And while it’s true that state and local elections officials can generally keep a copy of the source code, critics say they rarely employ computer programmers sophisticated enough to understand it. Quite the contrary: When a county buys touch-screen voting machines, its elections director becomes, as Warren Parish, a voting activist in Florida, told me, “the head of the largest I.T. department in their entire government, in charge of hundreds or thousands of new computer systems, without any training at all.” Many elections directors I spoke with have been in the job for years or even decades, working mostly with paper elections or lever machines. Few seemed very computer-literate.

The upshot is a regulatory environment in which, effectively, no one assumes final responsibility for whether the machines function reliably. The vendors point to the federal and state governments, the federal agency points to the states, the states

rely on the federal testing lab and the local officials are frequently hapless.

This has created an environment, critics maintain, in which the people who make and sell machines are now central to running elections. Elections officials simply do not know enough about how the machines work to maintain or fix them. When a machine crashes or behaves erratically on Election Day, many county elections officials must rely on the vendors — accepting their assurances that the problem is fixed and, crucially, that no votes were altered.

In essence, elections now face a similar outsourcing issue to that seen in the Iraq war, where the government has ceded so many core military responsibilities to firms like Halliburton and Blackwater that Washington can no longer fire the contractor. Vendors do not merely sell machines to elections departments. In many cases, they are also paid to train poll workers, design ballots and repair broken machines, for years on end.

“This is a crazy world,” complained Ion Sancho, the elections supervisor of Leon County in Florida. “The process is so under control by the vendor. The primary source of information comes only from the vendor, and the vendor has a conflict of interest in telling you the truth. The vendor isn’t going to tell me that his buggy software is why I can’t get the right time on my audit logs.”

As more and more evidence of machine failure emerges, senior government officials are sounding alarms as did the computer geeks of years ago over the growing role of private companies in elections. When I talked to Jennifer Brunner in October, she told me she wished all of Ohio’s machines were “open source” — that is, run on computer code that is published publicly, for anyone to see. Only then, she says, would voters trust it; and the scrutiny of thousands of computer scientists worldwide would ferret out any flaws and bugs.

On Nov. 6, the night of the Cuyahoga crashes, Jeff Hastings — the Republican head of the election board — sat and watched the Diebold technicians try to get the machines running. “Criminy,” he said. “You’ve got four different vendors. Why should their source codes be private? You’ve privatized the essential building block of the election system.”

The federal government appears to have taken that criticism to heart. New standards for testing voting machines now being implemented by the E.A.C. are regarded as more rigorous; some results are now being published online.

Amazingly, the Diebold spokesman, Chris Riggall, admitted to me that the company is considering making the software open source on its next generation of touch-screen machines, so that anyone could download, inspect or repair the code. The pressure from states is growing, he added, and “if the expectations of our customers change, we’ll have to respond to that reality.”

IF YOU WANT TO GET a sense of the real stakes in voting-machine politics, Christine Jennings has a map to show you. It is a sprawling, wall-size diagram of the voting precincts that make up Florida’s 13th district, and it hangs on the wall of her campaign office in Sarasota, where she ran for the Congressional seat in November 2006. Jennings, a Democrat, lost the seat by 369 votes to the Republican, Vern Buchanan, in a fierce fight to replace Katherine Harris. But Jennings quickly learned of an anomaly in the voting: some 18,000 people had “undervoted.” That is, they had voted in every other race — a few dozen were on the ballot, including a gubernatorial contest — but abstained in the Jennings-Buchanan fight. A normal undervote in any given race is less than 3 percent. In this case, a whopping 13 percent of voters somehow decided to not vote.

“See, look at this,” Jennings said, dragging me over to the map when I visited her in November. Her staff had written the size of the undervote in every precinct in Sarasota, where the undervotes occurred: 180 votes in one precinct, 338 in another. “I mean, it’s huge!” she said. “It’s just unbelievable.” She pointed to Precinct 150, a district on the south end of

Sarasota County. Buchanan received 346 votes, Jennings received 275 and the undervote was 133. “I mean, people would walk in and vote for everything except this race?” she said. “Why?”

Jennings says he believes the reason is simple: Sarasota’s touch-screen machines malfunctioned — and lost votes that could have tipped the election in her favor. Her staff has received hundreds of complaints from voters reporting mysterious behavior on the part of the machines. The specific model that Sarasota used was the iVotronic, by the company ES&S. According to the complaints, when voters tried to touch the screen for Jennings, the iVotronic wouldn’t accept it, or would highlight Buchanan’s name instead. When they got to the final pages of the ballot, where they reviewed their picks, the complainants said, the Jennings-Buchanan race was missing — even though they were sure they’d voted in it. The reports streamed in not merely from technophobic senior citizens but also from tech-savvy younger people, including a woman with a Ph.D. in computer science and a saleswoman who actually works for a firm that sells touch-screen devices. (Even Vern Buchanan’s wife reported having trouble voting for her husband.)

If the election had been in Cuyahoga, the paper trail might have settled the story. But the iVotronic, unlike Cuyahoga’s machines, does not provide a paper backup. It records votes only in digital memory: on a removable flash-memory card and on an additional flash-memory chip embedded inside the machine. Since the Jennings-Buchanan election was so close, state law called for an automatic recount. But on a paperless machine like the iVotronic, a recount is purely digital — it consists of nothing but removing the flash memory inside the machine and hitting “print” again. Jennings did, indeed, lose the recount; when they reprinted, elections workers found that the internal chips closely matched the original count (Jennings picked up four more votes). But for Jennings this is meaningless, because she says it was the screens that malfunctioned.

As evidence, she brandishes pieces of evidence she says are smoking guns. One is a memo from ES&S executives, issued in August 2006, warning that they had found a bug in the iVotronic software that produced a delay in the screen; after a voter made her choice, it would take a few seconds for the screen to display it. This, Jennings noted, could cause problems, because a voter, believing that the machine had not recorded her first touch, might push the screen again — accidentally deselecting her initial vote. Jennings also suspects that the iVotronic’s hardware may have malfunctioned. An August HDNet investigation by Dan Rather discovered that the company manufacturing the touchscreens for the iVotronic had a history of production flaws. The flaw affected the calibration of the screen: When exposed to humidity — much like the weather in Florida — the screen would gradually lose accuracy.

Elections officials in Sarasota and ES&S hotly disagree that the machines were in error, noting that the calibration problems with the screens were fixed before the election. Kathy Dent, Sarasota’s elections supervisor, suspects that the undervote was real — which is to say, voters intentionally skipped the race, to punish Jennings and Buchanan for waging a particularly vitriolic race. “People were really fed up,” she told me. Other observers say voters were simply confused by the ballot design and didn’t see the Jennings-Buchanan race.

To try to settle the question, a government audit tried to test whether the machines had malfunctioned. The state acquired a copy of the iVotronic source code from ES&S and commissioned a group of computer scientists to inspect it. Their report said they could find no flaws in the code that would lead to such a large undervote. Meanwhile, the state conducted a mock election, getting elections workers to repeatedly click the screens on iVotronic machines, voting Jennings or Buchanan. Again, no accidental undervote appeared. Early results from a separate test by an M.I.T. professor found that when voters were presented with the Sarasota ballot, over 16 percent accidentally skipped over the Jennings-Buchanan race — suggesting that poor ballot design and voter error was, indeed, part of the problem.

These explanations have not satisfied Jennings and her supporters. Kendall Coffey, one of Jennings's lawyers, has a different theory: the votes were mostly lost because of a "nonrecurring software bug" — a quirk that, like the sliding-finger bug, only crops up some of the time, propelled by voter actions that the audits did not replicate, like a voter's accidentally touching the screen in two places at once. For her part, Jennings brushes off the idea that voters were punishing her and Buchanan. Plenty of Congressional fights are nasty, she says, but they almost never yield 13 percent undervotes.

And on and on it goes. ES&S and Sarasota correctly point out that Jennings has no proof that a bug exists. Jennings correctly points out that her opponents have no proof a bug doesn't exist. This is the ultimate political legacy of touch-screen voting machines and the privatization of voting machinery generally. When invisible, secretive software runs an election, it allows for endless mistrust and muttered accusations of conspiracy. The inscrutability of the software — combined with touch-screen machines' well-documented history of weird behavior — allows critics to level almost any accusation against the machines and have it sound plausible. "It's just like the Kennedy assassination," Shamos, the Carnegie Mellon computer scientist, laments. "There's no matter of evidence that will stop people from spinning yarns."

Part of the problem stems from the fact that voting requires a level of precision we demand from virtually no other technology. We demand that the systems behind A.T.M.'s and credit cards be accurate, of course. But if they're not, we can quickly detect something is wrong: we notice that our balance is off and call the bank, or the bank notices someone in China bought $10,000 worth of clothes and calls us to make sure it's legitimate. But in an election, the voter must remain anonymous to the government. If a machine crashes and the county worries it has lost some ballots, it cannot go back and ask voters how they voted — because it doesn't know who they are. It is the need for anonymity that fuels the quest for perfection in voting machines.

Perfection isn't possible, of course; every voting system has flaws. So historically, the public — and candidates for public office — have grudgingly accepted that their voting systems will produce some errors here and there. The deep, ongoing consternation over touch-screen machines stems from something new: the unpredictability of computers. Computers do not merely produce errors; they produce errors of unforeseeable magnitude. Will people trust a system when they never know how big or small its next failure will be?

ON THE FRIDAY BEFORE the November elections in Pennsylvania, I wandered into a church in a suburb of Pittsburgh. The church was going to serve as a poll location, and I was wondering: Had the voting machines been dropped off? Were they lying around unguarded — and could anyone gain access to them?

When I approached the side door of the church at 6 p.m., two women were unloading food into the basement kitchen. (They were visitors from another church who had a key to get in, but they told me they'd found the door unlocked.) I held the door for them, chatted politely, then strolled into the otherwise completely empty building. Neither woman asked why I was there.

I looked over in the corner and there they were: six iVotronic voting machines, stacked up neatly. While the women busied themselves in their car, I was left completely alone with the machines. The iVotronics had been sealed shut with numbered tamper seals to prevent anyone from opening a machine illicitly, but cutting and resealing them looked pretty easy. In essence, I could have tampered with the machines in any way I wanted, with very little chance of being detected or caught.

Is it possible that someone could hack voting machines and rig an election? Elections officials insist that they are extremely careful to train poll workers to recognize signs of machines that had been tampered with. They also claim, frequently, that the machines are carefully watched. Neither is entirely true. Machines often sit for days before elections in churches, and while churches may be wonderfully convenient polling locations, they're about as insecure a location as you could imagine:

strangers are *supposed* to wander into churches. And while most poll workers do carefully check to ensure that the tamper seals on the machines are unbroken, I heard reports from poll workers who saw much more lax behavior in their colleagues.

Yet here's the curious thing: Almost no credible scientific critics of touch-screen voting say they believe any machines have ever been successfully hacked. Last year, Ed Felten, the computer scientist from Princeton, wrote a report exhaustively documenting the many ways a Diebold AccuVote-TSX could be hacked — including a technique for introducing a vote-rigging virus that would spread from machine to machine in a precinct. But Felten says the chance this has really happened is remote. He argues that the more likely danger of touch-screen machines is not in malice but in errors. Michael Shamos agrees. "If there are guys who are trying to tamper with elections through manipulation of software, we would have seen evidence of it," he told me. "Nobody ever commits the perfect crime the first time. We would have seen a succession of failed attempts leading up to possibly a successful attempt. We've never seen it."

This is a great oddity in the debate over electronic voting. When state officials in California and Ohio explain why they're moving away from touch-screen voting, they inevitably cite hacking as a chief concern. And the original, left-wing opposition to the machines in the 2004 election focused obsessively on Diebold's C.E.O. proclaiming that he would help "Ohio deliver its electoral votes" for Bush. Those fears still dominate the headlines, but in the real world of those who conduct and observe voting machines, the realistic threat isn't conspiracy. It's unreliability, incompetence and sheer error.

IF YOU WANTED to know where the next great eruption of voting-machine scandal is likely to emerge, you'd have to drive deep into the middle of Pennsylvania. Tucked amid rolling, forested hills is tiny Bellefonte. It is where the elections board of Centre County has its office, and in the week preceding the November election, the elections director, Joyce McKinley, conducted a public demonstration of the county's touch-screen voting machines. She would allow anyone from the public to test six machines to ensure they worked as intended.

"Remember, we're here to observe the machines, not debate them," she said dryly. The small group that had turned out included a handful of anti-touch-screen activists, including Mary Vollero, an art teacher who wore pins saying "No War in Iraq" and "Books Not Bombs." As we gathered around, I could understand why the county board had approved the purchase of the machines two years ago. For a town with a substantial elderly population, the electronic screens were large, crisp and far easier to read than small-print paper ballots. "The voters around here love 'em," McKinley shrugged.

But what's notable about Centre County is that it uses the iVotronic — the very same star-crossed machine from Sarasota. Given the concerns about the lack of a paper trail on the iVotronics, why didn't Centre County instead buy a machine that produces a paper record? Because Pennsylvania state law will not permit any machine that would theoretically make it possible to figure out how someone voted. And if a Diebold AccuVote-TSX, for instance, were used in a precinct where only, say, a dozen people voted — a not-uncommon occurrence in small towns — then an election worker could conceivably watch who votes, in what order, and unspool the tape to figure out how they voted. (And there are no alternatives; all touch-screen machines with paper trails use spools.) As a result, nearly 40 percent of Pennsylvania's counties bought iVotronics.

Though it has gone Democratic in the last few presidential elections, Pennsylvania is considered a swing state. As the political consultant James Carville joked, it's a mix of red and blue: you've got Pittsburgh and Philadelphia at either end and Alabama in the middle.

It also has 21 electoral-college votes, a relatively large number that could decide a tight presidential race. Among election-machine observers, this provokes a shudder of anticipation. If the presidential vote is close, it could well come

down to a recount in Pennsylvania. And a recount could uncover thousands of votes recorded on machines that displayed aberrant behavior — with no paper trail. Would the public accept it? Would the candidates? As Candice Hoke, the head of Ohio's Center for Election Integrity, puts it: "If it was Florida in 2000 and Ohio in 2004, everyone is saying it's going to be Pennsylvania in 2008."

The prospect of being thrust into the national spotlight has already prompted many counties to spar over ditching their iVotronics. The machines were an election issue in Centre County in November, with several candidates for county commissioner running on a pledge to get rid of the devices. (Two won and are trying to figure out if they can afford it.) And the opposition to touch-screens isn't just coming from Democrats. When the Pennsylvania Republican Rick Santorum lost his Senate seat in 2006, some Santorum voters complained that the iVotronics "flipped" their votes before their eyes. In Pittsburgh, the chief opponent of the machines is David Fawcett, the lone Republican on the county board of elections. "It's not a partisan issue," he says. "And even if it was, Republicans, at least in this state, would have a much greater interest in accuracy. The capacity for error is big, and the error itself could be so much greater than it could be on prior systems."

GIVEN THAT THERE IS NO perfect voting system, is there at least an optimal one? Critics of touch-screen machines say that the best choice is "optical scan" technology. With this system, the voter pencils in her vote on a paper ballot, filling in bubbles to indicate which candidates she prefers. The vote is immediately tangible to the voters; they see it with their own eyes, because they personally record it. The tallying is done rapidly, because the ballots are fed into a computerized scanner. And if there's a recount, the elections officials can simply take out the paper ballots and do it by hand.

Optical scanning is used in what many elections experts regard as the "perfect elections" of Leon County in Florida, where Ion Sancho is the supervisor of elections. In the late '80s, when the county was replacing its lever machines, Sancho investigated touch-screens. But he didn't think they were user-friendly, didn't believe they would provide a reliable recount and didn't want to be beholden to a private-sector vendor. So he bought the optical-scanning devices from Unisys and trained his staff to be able to repair problems when the machines broke or malfunctioned. His error rate — how often his system miscounts a ballot — is three-quarters of a percent at its highest, and has dipped as low as three-thousandths of a percent.

More important, his paper trail prevents endless fighting over the results of tight elections. In one recent contest, a candidate claimed that his name had not appeared on the ballot in one precinct. So Sancho went into the Leon County storage, broke the security seals on the records, and pulled out the ballots. The name was there; the candidate was wrong. "He apologized to me," Sancho recalls. "And that's what you can't do with touch-screen technology. You never could have proven to that person's satisfaction that the screen didn't show his name. I like that certainty. The paper ends the discussion." Sancho has never had a legal fight over a disputed election result. "The losers have admitted they lost, which is what you want," he adds. "You have to be able to convince the loser they lost."

That, in a nutshell, is what people crave in the highly partisan arena of modern American politics: an election that can be extremely close and yet regarded by all as fair. Not only must the losing candidate believe in the loss; the public has to believe in it, too.

This is why Florida's governor, Charlie Crist, stung by the debacle in Sarasota, persuaded the state to abandon its iVotronic machines before the 2008 presidential elections and adopt optical scanning; and why, in Ohio, Cuyahoga County is planning to spend up to $12 million to switch to optical scanning in the next year (after the county paid $21 million for its touch-screens just a few years ago).

Still, optical scanning is hardly a flawless system. If someone doesn't mark a ballot clearly, a recount can wind up back in

the morass of arguing over “voter intent.” The machines also need to be carefully calibrated so they don’t miscount ballots. Blind people may need an extra device installed to help them vote. Poorly trained poll workers could simply lose ballots. And the machines do, in fact, run software that can be hacked: Sancho himself has used computer scientists to hack his machines. It’s also possible that any complex software isn’t well suited for running elections. Most software firms deal with the inevitable bugs in their product by patching them; Microsoft still patches its seven-year-old Windows XP several times a month. But vendors of electronic voting machines do not have this luxury, because any update must be federally tested for months.

There are also serious logistical problems for the states that are switching to optical scan machines this election cycle. Experts estimate that it takes at least two years to retrain poll workers and employees on a new system; Cuyahoga County is planning to do it only three months. Even the local activists who fought to bring in optical scanning say this shift is recklessly fast — and likely to cause problems worse than the touch-screen machines would. Indeed, this whipsawing from one voting system to the next is another danger in our modern electoral wars. Public crises of confidence in voting machines used to come along rarely, every few decades. But now every single election cycle seems to provoke a crisis, a thirst for a new technological fix. The troubles of voting machines may subside as optical scanning comes in, but they’re unlikely to ever go away.

Clive Thompson, a contributing writer for the magazine, writes frequently about technology.