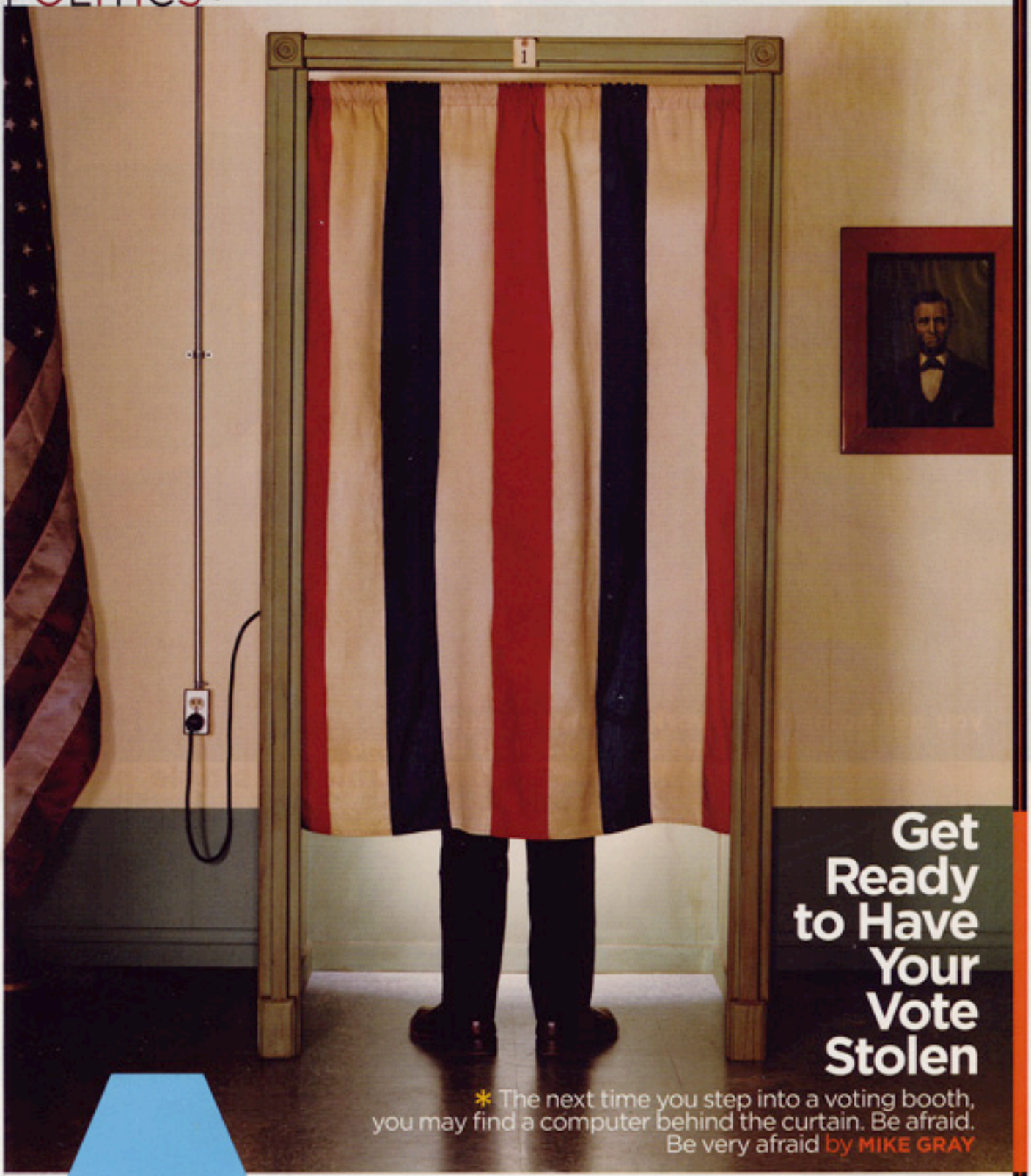


Get Ready to Have Your Vote Stolen

* The next time you step into a voting booth, you may find a computer behind the curtain. Be afraid. Be very afraid by MIKE GRAY

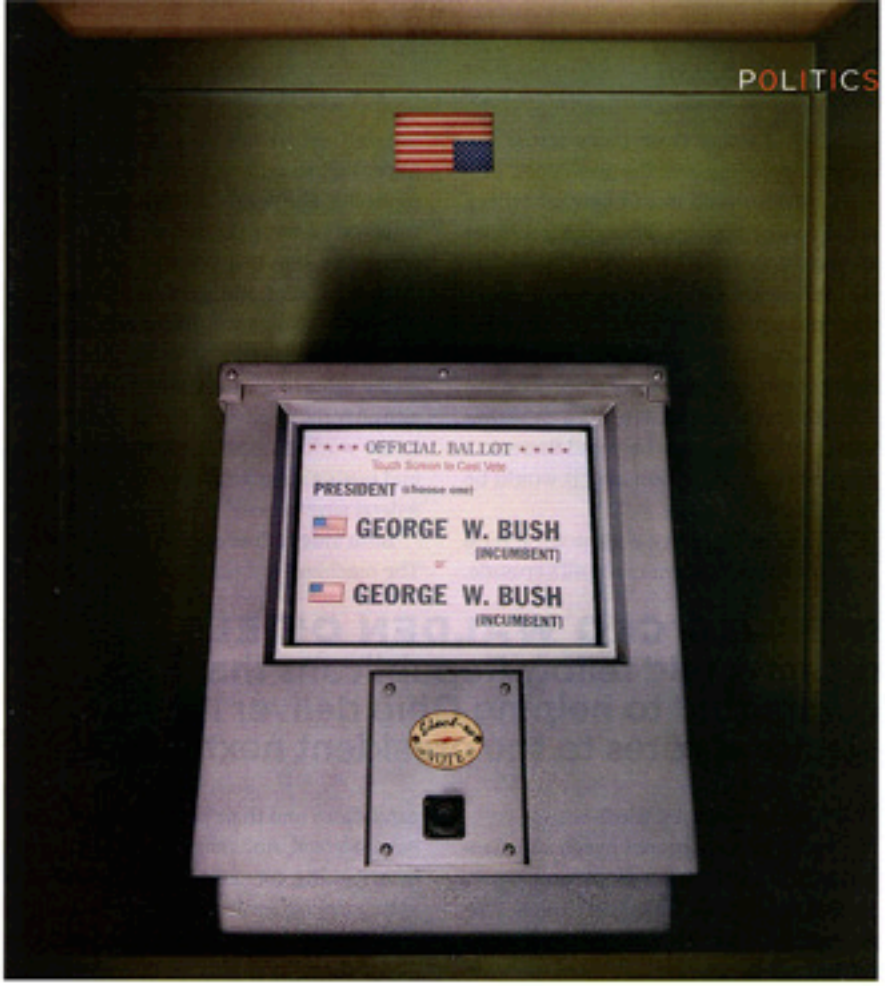
ATLANTA, NOVEMBER 5, 2002—Before this election day is over, the city will be drenched with an inch and a half of rain, and that's not good news for the Democrats. Conventional wisdom says a low turnout favors the GOP. On the other hand, the polls have been giving the Democrats plenty of breathing room. Senator Max Cleland has been well in front of Republican challenger Saxby Chambliss in every head count so far, and incumbent Democratic governor Roy Barnes has an eleven-point lead over Republican Sonny Perdue.

But when the polls close at 7 P.M., the Democrats are knocked off their feet by the initial returns. The Republican ticket immediately breaks out in front, and as the night wears on, the lead only increases. It is a stunning upset. For the first time "since the invention of the telephone," Georgia will have a Republican governor; Perdue has defeated Barnes in a whopping turnaround from last week's polls. Cleland goes down by a similar count. The sheer magnitude of the reversal leaves everyone reeling. Says Republican pollster Whit Ayres, "I know of no one's polling that predicted this or *(continued on page 267)*

Photographs by **DAN WINTERS**

saw it coming." But state GOP chairman Ralph Reed, the man who will take credit for this astonishing victory, has a ready explanation. On the Saturday before the election, Reed and his colleagues dispatched nine busloads of volunteers into white rural and suburban Republican strongholds in a last-minute get-out-the-vote campaign.

Reed's explanation makes sense until you look at the actual numbers. It turns out there was no dramatic shift in the color of the 2002 vote. Blacks and whites came to the polls in almost exactly the same ratio they had four years earlier. The county-by-county breakdown is equally unsettling. When the stats are examined in detail by a team from the *Baltimore City Paper*, they find an extraordinary change of heart between the primary and the general election. For some reason, the counties that contain about 60 percent of the Georgia electorate decided to switch sides. What's more, says reporter Van Smith, these shifts occurred in unlikely areas of the state. In the bedrock Democratic southern counties, Cleland still won, but Chambliss picked up 22 percent more ballots than he could have expected, based on the primary.



"A LOT OF BAD STUFF HAPPENED in Georgia. The programmers had to do last-minute software patches on all 22,000 machines."

Now alarm bells are going off, and around the country professional election watchers are snapping to attention, because this was no ordinary election. This was the first totally computerized contest, the first statewide ballot conducted exclusively on touch-screen DREs, or "direct-recording electronic" devices.

* * * * * *

IN THE AFTERMATH of the blighted 2000 presidential election, public attention was focused on the mechanics of voting at a moment when that industry was undergoing a tectonic shift. The paper ballot was about to be replaced by computers. Last year, as part of the Help America Vote Act, Congress appropriated $3.9 billion to aid local election boards in making the transition to twenty-first-century technology, and this ignited a feeding frenzy among the manufacturers of electronic voting machinery. The next time you step into a polling booth, there's a good chance you'll be looking at one of these devices.

The new touch-screen ballot works something like an automated teller machine, and in fact one of the major suppliers of electronic voting equipment is Diebold Incorporated, a leading manufacturer of ATMs. Diebold Election Systems sold Georgia the 22,000 DREs used in the 2002 election. These machines have impressive advantages over anything we've seen before: They are chad-free, the results are available instantly, and, like ATMs, they can be programmed to speak your language. If you make a mistake, the computer tells you how to fix it.

However, electronic voting requires a leap of faith. Not one person in a thousand has any idea what actually goes on inside the circuits of an ATM, yet we touch the screen and take the cash with casual confidence in the bookkeeping. Since counting votes is arguably more important than counting money, one question immediately comes to mind: When I touch the square for "Abe Lincoln," how do I know the computer didn't actually store my vote under "McClellan"?

To guard against this, all new designs are tested by independent laboratories where the machines and their software are scrutinized in detail. State and local officials run their own extensive accuracy tests, complete with mock elections. The hardware itself is either under lock and key or within eyesight of election officials at all times to prevent unauthorized access.

But to Professor David Dill, a Stanford University computer scientist, this is all just window dressing. Dill, a self-described propeller-head, is an expert in the field of computer verification—the science of figuring out whether a system is doing what it's supposed to be doing. He believes not only that the DREs are vulnerable to being rigged but that it would also be relatively easy to insert a corrupt "Trojan horse" program that would alter a whole state election like—say, Georgia's. "If you talk to the real experts," says Dill, "they'll tell you these machines are claiming to do something that, with the technology they're using, is effectively impossible."

What concerns Dill is that the election officials who are buying these machines don't have an adequate grasp of the dark side of computer programming. "There is no evidence that anybody who knows anything about computer security has looked at any part of these systems," he says. Dill's colleague David Jefferson, of Lawrence Livermore National Laboratory, has an even more sobering take. "Almost certainly 1 or 2 percent...of all votes cast nationally on a particular vendor's equipment could be switched without detection, changing the

outcome of many close races across the country, including even the presidency."

An attack would most likely take place at the vendor's factory, where the machines are assembled and programmed. "By far the easiest mode of attack is to tamper with the software while it is in development," says Jefferson. In this scenario, a single corrupt programmer at work on the operating system could insert a code that would shift a few votes here and there on a random basis. Jefferson says it would be virtually undetectable.

This chilling insight has attracted several hundred fellow academics to Dill's crusade. The roster is almost a who's who of computer-science-department heads and associates from M.I.T., Johns Hopkins, Cornell, Princeton, Cal Tech, Carnegie Mellon, Purdue, Berkeley and Penn State—all leading technologists who are alarmed by what they fear is sloppy engineering encased in a shroud of secrecy.

"If you try to find out anything about the inspection process or how the machines work," says Dill, "you're met with the answer 'It's proprietary; we have to keep that secret.'" The manufacturers' obsession with secrecy is understandable. If a competitor steals the operating software, it could be a commercial disaster. Unfortunately, this need for security means that nobody is allowed to see the source code other than the original programmers and the people at the independent lab who certified it.

For scholars like Dill who read software programs like the morning paper, that's not good enough. "Computer security's incredibly hard," he says, "and unless somebody has done a very meticulous analysis of these systems, there's always a hole. In fact, maybe there's always a hole anyway."

On the other side of this argument are a number of experienced election officials who think Dill and Jefferson are ivory-tower theorists with no practical understanding of how an actual election is run. For Mischelle Townsend, registrar of voters for Riverside County, California, security is not an abstraction. It's something she lives with daily—labyrinthine checks and balances, each move dictated by volumes of regulations and scrutinized by all contenders. She's convinced that the new DREs she just bought from Sequoia Voting Systems are not only secure but more secure than the paper ballots and optical scanners they're replacing. She points out that the manufacturer has no way of knowing where a particular candidate is going to appear on the electronic ballot, and she scoffs at the possibility of an undetected Trojan horse embedded in the system. "The skeptics aren't giving value to the tests we're having before and after the election," she says. "No country in the world has the rigorous certification and testing standards of California and the federal government."

Both sides agree on one thing, at least: The machines are very vulnerable *after* the candidates and their ballot positions have been selected. And that's one reason for the interlocking security that surrounds all voting machinery in the run-up to Election Day. No system is perfect, however, and one of the most glaring weaknesses in electronic voting came to light, curiously, during the recent election in Georgia.

DIEBOLD CEO WALDEN O'DELL recently told fellow Republicans that he is "committed to helping Ohio deliver its electoral votes to the president next year."

* * * * * *

"A LOT OF BAD STUFF happened in Georgia," says Dill. "The machines weren't working very well, and the programmers had to do some last-minute software patches on all 22,000 machines in the state. That's a bad situation. They didn't have a chance to retest the software." These preelection glitches were certainly understandable. Before Diebold struck it rich in Georgia, the company had been selling its new DREs pretty much one county at a time. Suddenly, it had to supply a whole state, and the factory was clearly straining.

According to Rob Behler, an installation technician employed by one of Diebold's subcontractors, there were quality-control problems from the outset. A quarter of the machines simply wouldn't function, and the software displayed "sporadic behavior." But in their mad dash to the finish line, Diebold's technical crews managed to pull it all together and save the day. The touch-screen machines were a smash hit with the voters, and Election Day problems turned out to be minimal.

But all this came at a price. For example, the final software fix had to be installed less than six weeks before the election on every machine in the state. "If I were going to hack an election," says Dill, "I would contrive a reason to distribute software at the last minute."

The fact that the software had been patched repeatedly in the months before the election came to light by accident early this year. Bev Harris, a Seattle author digging into the issue for a book on electronic voting, found a memo from the Georgia secretary of state's office dated six weeks before the election. Press secretary Chris Riggall, responding to a critic, wrote, "Diebold programmers developed a patch which was applied to the units deployed in Hall and Marion counties.... That is now occurring to all units in all counties."

Although Diebold initially denied any knowledge of the patch, the company now admits that changes were made to the software in June, July and September. It insists that these changes were insignificant modifications to the Windows CE 3.0 operating system and that the company never touched the actual election software, which is a totally separate program.

The problem is, whatever these changes were, they were apparently done on the fly without being run through the certification process that is at the heart of the whole security system. According to Britain Williams, who oversaw the technical evaluation of Georgia's DREs, "Any change to either the Microsoft operating system or the Diebold election system voids the state certification. The revised system must then go back through the entire state-certification process." If Diebold had actually done that, of course, the installation would have come to a screeching halt, and that was out of the question. "We had 186 days from the time Diebold signed the contract till we had to run an election," says Williams. So election officials apparently decided to skip the certification formalities and get on with it.

An emeritus professor at Georgia's Kennesaw State University, Williams, like Dill, is a computer scientist, but he's staunchly on the other side of the argument. He insists that the patches, whether certified or not, could not possibly have altered the operation of the election software because they were just minor adjustments to the Windows operating system.

Yet the process by which these updates are administered to the individual voting machines leaves a lot of room for maneuvering. For example, when the Diebold factory programmers create a new fix, they don't just send out the patch; they send out a whole new version of the software with the patch installed. In other words, the machine is completely reprogrammed every time the slightest change is made.

And to Davis Jefferson, this is a disaster waiting to happen. "With vendor insider attacks, it is actually easier to attack statewide races than local races and easier to attack national races than statewide races," he says. "All it requires is one corrupt programmer in a position to edit the code base. His or her malicious code will be transported and loaded into thousands of machines during upgrades, bug fixes or other standard software modifications so that the tainted code is loaded onto the chips through the regular management channels." In other words, the future of the Republic could be in the hands of a single individual who happens to be ideologically motivated or short of cash.

* * * * * *

IF THE GREATEST THREAT posed by DREs lies within the labs and factories where they are built, then the question is begged: Who exactly are these voting-machine vendors, and what do we know about them? Not much, it turns out. Bev Harris has spent several hundred hours researching this question for her book, *Black Box Voting*, and she found herself wading through a convolution of mergers, cross-ownership, family relations and mystery.

Harris has at least been able to sketch the outlines. The lion's share of the market is controlled by three outfits: Election Systems & Software (ES&S), Diebold and Sequoia. ES&S was started in the early '80s by two brothers, Todd and Bob Urosevich, with funding from the *Omaha World Herald* and the politically conservative Ahmanson family. In 1993, Bob Urosevich left ES&S to start his own company, which merged with another outfit and was moved to McKinney, Texas. Enter Diebold, the Ohio-based ATM giant, which bought Bob Urosevich's company in January 2002 but left him and the voting-machine operation in McKinney. The Urosevich brothers are now major players at two of the big three. The third contender, Sequoia Voting Systems of Oakland, California, is foreign owned.

Within this opaque collection of organizations, researchers have been able to connect a few dots, and they reveal astounding opportunities for conflict of interest. Near the top of the list would be Diebold CEO Walden O'Dell, a major fund-raiser for the Bush 2004 reelection campaign, who recently told fellow Republicans that he is "committed to helping Ohio deliver its electoral votes to the president next year."

Then there's Senator Chuck Hagel of Nebraska, who owns an interest in the ES&S voting machines that elected him in 1998 and 2002. In fact, Hagel moved to Omaha in the first place to work for ES&S. When Bob Urosevich left to start his competing business, Chuck Hagel took over as CEO. Hagel later resigned to run for office, but he and campaign treasurer Michael R. McCarthy are still significant shareholders.

Conspiracy theorists, not surprisingly, point out that the 2002 Georgia and Nebraska elections carried with them control of the Senate. But whether or not there was anything sinister afoot is something we will never know. There simply isn't any way to find out. There are no paper ballots to examine, and if you ask a DRE for a recount, it will just spit out exactly the same numbers it gave you before. Without an independent verification of some kind, you have no way of knowing that the votes were stored properly in the first place.

That's what Dill and his fellow propeller-heads are ultimately after: a paper trail. They are not opposed to computerized voting. In fact, security concerns aside, they love the idea. They just want the manufacturers to add one little feature: a printer that will produce a paper copy of the ballot. That's all there is to it. This relatively simple step, they say, makes electronic voting manageable, because the voter gets to verify a hard copy that goes to a vault and is used only for a recount. If you do have a recount, you can look at physical ballots the voter has seen and approved. You don't have to settle for something stored on a circuit board.

This idea seems so logical to Representative Rush Holt, a third-term Democrat from New Jersey, that he has introduced legislation to make printers mandatory on DREs. Naturally, the voting-machine proponents are mounting a counterattack, and election officials like Mischelle Townsend are against the idea as well. Townsend opposes printers because of the practical problems—additional expense, redundancy and the fact that "they're always jamming with paper"—which could truly turn into an Election Day nightmare.

However, for David Dill and other top computer scientists, the bottom line is this: Either we install a voter-verifiable independent audit trail or we are at the mercy of unelected technocrats. "Using these machines is tantamount to handing complete control of vote counting to a private company," says Dill. "These machines represent a serious threat to democracy."

MIKE GRAY *is a journalist and filmmaker based in Los Angeles. This is his first piece for* GQ.