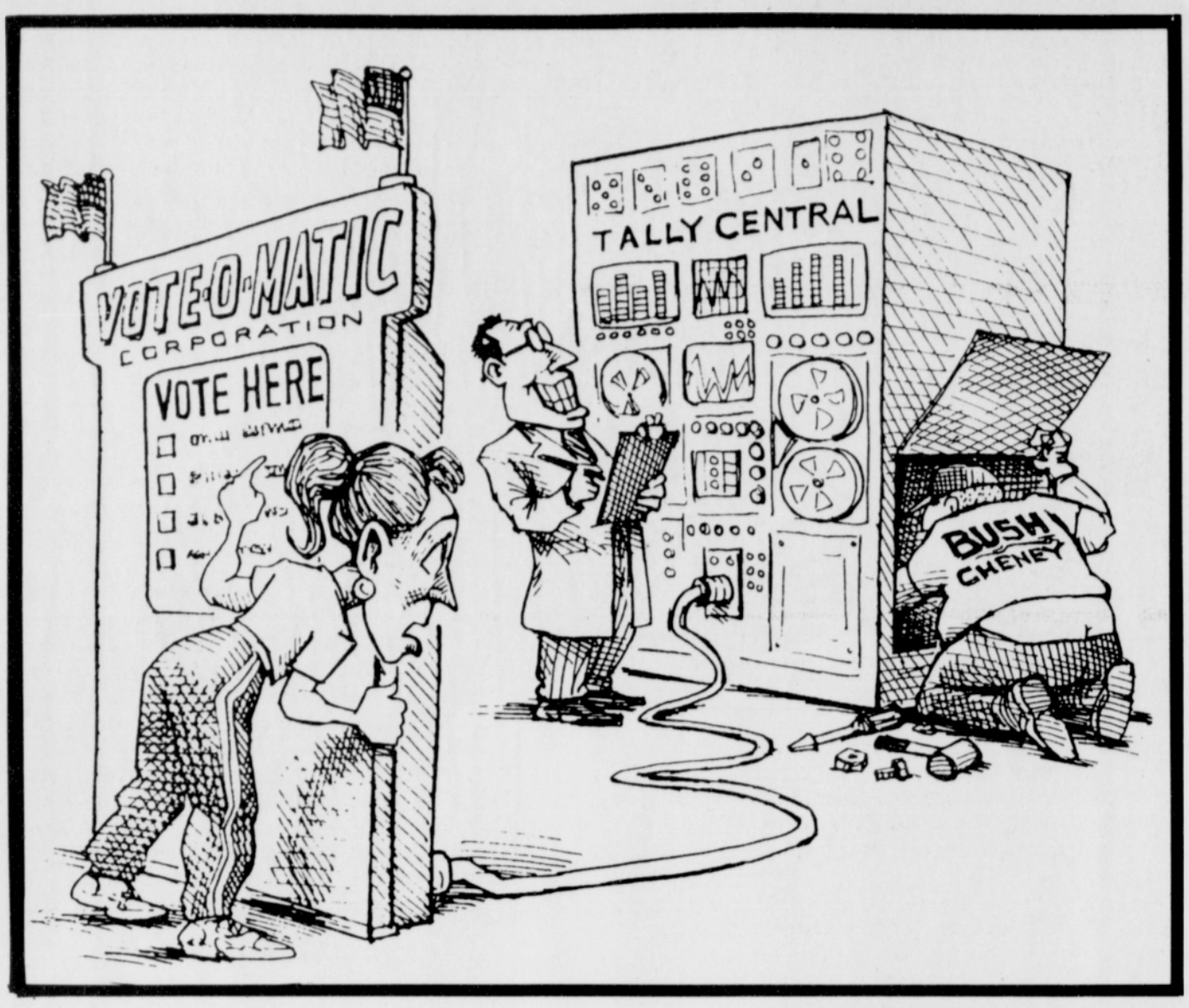
ALL THE PRESIDENT'S VOTES?



DRAWINGS BY MATT WUERKER

BY ANDREW GUMBEL

Something very odd happened in the mid-term elections in Georgia in November 2002. On the eve of the vote, opinion polls showed Roy Barnes, the incumbent Democratic governor, leading by between 9 and 11 points. In a somewhat closer keenly watched Senate race, polls indicated that Max Cleland, the popular Democrat up for re-election, was ahead by 2 to 5 points against his Republican challenger, Saxby Chambliss.

Those figures were more or less what political experts would have expected in a state with a long tradition of electing Democrats to statewide office. But then the results came in, and all of Georgia appeared to have been turned upside down. Barnes lost the governorship to the Republican, Sonny Perdue, 46% to 51%, a swing of as much as 16 percentage points from the last opinion polls. Cleland lost to Chambliss 46% to 53%, a last minute swing of 9 to 12 points.

Red-faced opinion pollsters suddenly had a lot of explaining to do and launched internal investigations. Political analysts credited the upset — part of a pattern of Republican successes around the country — to a huge campaigning push by President Bush in the final days of the race. They also said that Roy Barnes had lost because of a surge of "angry white men" punishing him for eradicating all but a vestige of the old confederate symbol from the state flag.

But something about these explanations did not make sense, and they have made even less sense over time. When the Georgia secretary of state's office published its demographic breakdown of the election in early 2003, it turned out there was no surge of angry white men; in fact, the only subgroup showing even a modest increase in turnout was black women.

There were also big, puzzling swings in partisan loyalties in different parts of the state.In 58 counties the vote was broadly in line with the primary election. In 27 counties in Republican-dominated north Georgia, however, Max Cleland unaccountably scored 14% points higher than he had in the primaries. And in 74 counties in the Democrat south, Saxby Chambliss garnered a whopping 22 points more for the Republicans than the party as a whole had won less than three months earlier.

Now, weird things like this do occasionally occur in elections, and the figures on their own are not proof of anything except statistical anomalies worthy of further study. But in Georgia there was an extra reason to be suspicious. The state became the first in the country that November to conduct an election entirely with touchscreen voting machines, after lavishing $45 million on a new system that promised to deliver the securest, most up-to-date, most voter-friendly election in the history of the republic. The machines, however, turned out to be anything but reliable. With academic studies showing the Georgia touchscreens to be poorly programmed, full of security holes and prone to tampering, and with thousands of similar machines from different companies being introduced at high speed across the country, computer voting may, in fact, be U.S. democracy's own 21st century nightmare.

In many Georgia counties the machines froze up, causing long delays as technicians tried to reboot them. In heavily Democratic Fulton County, in downtown Atlanta, 67 memory cards from the voting machines went missing, delaying certification of the results for 10 days. In neighboring DeKalb County, 10 memory cards were unaccounted for; they were later recovered from terminals that had supposedly broken down and taken out of service.

It is still unclear exactly how results from these missing cards were tabulated, or if they were counted at all. And we will probably never know, for a highly disturbing reason. The vote count was not conducted by state election officials, but by the private company that sold Georgia the voting machines in the first place, under a strict trade-secrecy contract that made it not only difficult but actually illegal — on pain of stiff criminal penalties — for the state to touch the equipment or examine the proprietary software to ensure the machines worked properly. There was not even a paper trail to follow up. The machines were fitted with thermal printing devices that could theoretically provide a written record of voters' choices, but these were not activated. Consequently, recounts were impossible. Had Diebold Inc., the manufacturer, been asked to review the votes, all it could have done was program the computers to spit out the same data as before, flawed or not.

Astonishingly these are the terms under which America's top three computer voting machine manufacturers — Diebold, Sequoia and Election Systems & Software (ES&S) — have sold their products to election officials around the country. Far from questioning the need for rigid trade secrecy and the absence of a paper record, secretaries of state and their technical advisers — anxious to banish memories of the hanging chad fiasco and other associated disasters in the 2000 Presidential recount in Florida — have, for the most part, welcomed the touchscreen voting machines as a technological miracle solution.

Georgia was not the only state in November 2002 to see last-minute swings in voting patterns. There were others in Colorado, Minnesota, Illinois and New Hampshire — all in races flagged as key partisan battlegrounds, and all won by the Republican Party. Again, this was widely attributed to campaigning efforts of President Bush and the demoralization of a Democratic Party too timid to speak out against the looming war in Iraq.

Strangely, however, the pollsters made no comparable howlers in lower-key races whose outcome was not seriously contested. Another anomaly, perhaps. What then is one to make of the fact that the owners of the three major computer voting machines are all prominent Republican Party donors? Or of a recent political fund-raising letter written to Ohio Republicans by Walden O'Dell, Diebold's chief executive, in which he said he was "committed to helping Ohio to deliver its electoral votes to the President (in 2004)" — even as his company was bidding for the contract on the state's new voting machinery?

Alarmed and suspicious, a group of Georgia citizens began to look into the November 2002 election to see whether there was any chance the results might have been deliberately or accidentally manipulated. Their research proved unexpectedly, and disturbingly, fruitful.

First, they wanted to know if the software had undergone adequate checking. Under state and federal law, all voting machinery and component parts must be certified before use in an election. So Atlanta graphic designer Dennis Wright wrote to the secretary of state's office for a copy of the certificate letter. Clifford Tatum, assistant director of legal affairs for the election division, wrote back, "We have determined that no records exist in the Secretary of State's office regarding a certification letter from the lab certifying the version of software used on Election Day." Mr. Tatum said it was possible the relevant documents were with Gary Powell, an official at the Georgia Technology Authority, so campaigners wrote to him as well. Mr. Powell responded he was "not sure what you mean by the words 'please provide written certification documents.'"

"If the machines were not certified, then right there the election was illegal," Mr. Wright says. The secretary of state's office has yet to demonstrate anything to the contrary. The investigating citizens then considered the nature of the software itself. Shortly after the election, Diebold technician Rob Behler came forward and reported that, when the machines were about to be shipped to Georgia polling stations in the summer of 2002, they performed so erratically their software had to be amended with a last-minute "patch." Instead of being transmitted via disk — a potentially time-consuming process, especially since its author was in Canada, not Georgia — the patch was posted, along with the entire election software package, on an open-access FTP, or file transfer protocol site, on the Internet.

That, according to computer experts, was a violation of the most basic of security precautions, opening all sorts of possibilities for the introduction of rogue or malicious code. At the same time, however, it gave campaigners a golden opportunity to circumvent Diebold's own secrecy demands and see exactly how the system worked. Roxanne Jekot, a computer programmer with 20 years experience and an occasional teacher at Lanier Technical College northeast of Atlanta, did a line-by-line review and found "enough to stand your hair on end."

"There were security holes all over it," she says, "from the most basic display of the ballot on the screen all the way through the operating system." Although the program was designed to be run on the Windows 2000 NT operating system, which has numerous safeguards to keep out intruders, Ms. Jekot found it worked just fine on the much less secure Windows 98; the 2000 NT security features were, as she put it, "nullified."

Also embedded in the software were the comments of the programmers working on it. One described what he and his colleagues had just done as "a gross hack." Elsewhere was the remark: "This doesn't really work." "Not a confidence builder, would you say?" Ms. Jekot says. "They were operating in panic mode, cobbling together something that would work for the moment, knowing that at some point they would have to go back to figure out how to make it work more permanently." She found some of the code downright suspect — for example, an overtly meaningless instruction to divide the number of write-in votes by 1. "From a legal standpoint there is absolutely no reason to do that," she says. "It raises an immediate red flag."

Mostly, though, she was struck by the shoddiness of much of the programming. "I really expected to have some difficulty reviewing the source code because it would be at a higher level than I am accustomed to," she says. "In fact, a lot of this stuff looked like the homework my first-year students might have turned in." Diebold had no specific comment on Ms.Jekot's interpretations, offering only a blanket caution about the complexity of election systems "often not well understood by individuals with little real-world experience."

But Ms. Jekot was not the only one to examine Diebold software and find it lacking. In July 2003, a group of researchers from the Information Security Institute at Johns Hopkins University in Baltimore discovered what they called "stunning flaws." These included putting the password in the source code, a basic security no-no; manipulating the voter smart-card function so one person could cast more than one vote; and other loopholes that could theoretically allow voters' ballot choices to be altered without their knowledge, either on the spot or by remote access.

Diebold issued a detailed response, saying the Johns Hopkins report was riddled with false assumptions, inadequate information and "a multitude of false conclusions." Substantially similar findings, however, were made in a follow-up study on behalf of the state of Maryland, in which a group of computer security experts catalogued 328 software flaws, 26 of them critical, putting the whole system "at high risk of compromise." "If these vulnerabilities are exploited, significant impact could occur on the accuracy, integrity, and availability of election results," their report says.

Ever since the Johns Hopkins study, Diebold has sought to explain away the open FTP file as an old, incomplete version of its election package. The claim cannot be independently verified because of the trade-secrecy agreement, and not everyone is buying it. "It is documented throughout the code who changed what and when. We have the history of this program from 1996 to 2002," Ms. Jekot says. "I have no doubt this is the software used in the elections." Diebold now says it has upgraded its encryption and password features — but only on its Maryland machines.

A key security question concerned compatibility with Microsoft Windows, and Ms. Jekot says just three programmers, all of them senior Diebold executives, were involved in this aspect of the system. One of these, Diebold's vice-president of research and development, Talbot Iredale, wrote an e-mail in April 2002 — later obtained by the campaigners — making it clear that he wanted to shield the operating system from Wylie Labs, an independent testing agency involved in the early certification process.

The reason that emerges from the e-mail is that he wanted to make the software compatible with WinCE 3.0, an operating system used for handhelds and PDAs; in other words, a system that could be manipulated from a remote location. "We do not want Wyle(*sic*)reviewing and certifying the operating systems," the e-mail says."Therefore can we keep to a minimum the references to the WinCE 3.0 operating system."

In an earlier intercepted e-mail, this from Ken Clark in Diebold's research and development department, the company explained upfront to another independent testing lab that the supposedly secure software system could be accessed without a password, and its contents easily changed using the Microsoft Access program. Mr. Clark says he had considered putting in a password requirement to stop dealers and customers from doing "stupid things," but that the easy access had often "got people out of a bind." Astonishingly, the representative from the independent testing lab did not see anything wrong with this and granted certification to the part of the software program she was inspecting — a pattern of lackadaisical oversight that was replicated all the way to the top of the political chain of command in Georgia, and in many other parts of the country.

Diebold has not contested authenticity of the e-mails, now openly accessible on the Internet. However, Diebold did caution that, as the e-mails were taken from a Diebold Election