The Independent | *http://news.independent.co.uk/world/americas/story.jsp?story=452972* 14 October 2003

All the President's votes?

A quiet revolution is taking place in US politics. By the time it's over, the integrity of elections will be in the unchallenged, unscrutinised control of a few large – and pro-Republican – corporations. Can democracy in America survive?

by Andrew Gumbel

Something very odd happened in the mid-term elections in Georgia last November. On the eve of the vote, opinion polls showed Roy Barnes, the incumbent Democratic governor, leading by between nine 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 two to five 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 per cent to 51 per cent, a swing of as much as 16 percentage points from the last opinion polls. Cleland lost to Chambliss 46 per cent 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 earlier this year, 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 percentage 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. Last November, the state became the first in the country to conduct an election entirely with touchscreen voting machines, after lavishing $54m (£33m) 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 US democracy's own 21st-century nightmare.

In many Georgia counties last November, 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 there for 10 days. In neighbouring DeKalb County, 10 memory cards were

unaccounted for; they were later recovered from terminals that had supposedly broken down and been 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 elections 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 programme 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 and 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 last November to see big last-minute swings in voting patterns. There were others in Colorado, Minnesota, Illinois and New Hampshire—all in races that had been flagged as key partisan battlegrounds, and all won by the Republican Party. Again, this was widely attributed to the campaigning efforts of President Bush and the demoralisation 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 next year"—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 last November's 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 an Atlanta graphic designer called Denis Wright wrote to the secretary of state's office for a copy of the certification 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, a Diebold technician called 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 that 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 programme 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 logical 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 the Diebold software and find it lacking. In July, 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 that 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 programme 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 reads. "Therefore can we keep to a minimum the references to the WinCE 3.0 operating system."

In an earlier intercepted e-mail, this one 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 programme. Mr Clark says he had considered putting in a password requirement to stop dealers and customers 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 programme 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 the 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 systems website in March 2003 by an illegal hack, the nature of the information stolen could have been revised or manipulated.

There are two reasons why the United States is rushing to overhaul its voting systems. The first is the Florida débâcle in the Bush-Gore election; no state wants to be the centre of that kind of attention again. And the second is the Help America Vote Act (HAVA), signed by President Bush last October, which promises an unprecedented $3.9bn (£2.3bn) to the states to replace their old punchcard-and-lever machines. However, enthusiasm for the new technology seems to be motivated as much by a bureaucratic love of spending as by a love of democratic accountability. According to Rebecca Mercuri, a research fellow at Harvard's John F Kennedy School of Government and a specialist in voting systems, the shockingly high error rate of punchcard machines (3-5 per cent in Florida in 2000) has been known to people in the elections business for years. It was only after it became public knowledge in the last presidential election that anybody felt moved to do anything about it.

The problem is, computer touchscreen machines and other so-called DRE (direct recording electronic) systems are significantly less reliable than punchcards, irrespective of their vulnerability to interference. In a series of research papers for the Voting Technology Project, a joint venture of the prestigious Massachussetts and California Institutes of Technology, DREs were found to be among the worst performing systems. No method, the MIT/CalTech study conceded, worked more reliably than hand-counting paper ballots—an option that US electoral officials seem to consider hopelessly antiquated, or at least impractical in elections combining multiple local, state and national races for offices from President down to dogcatcher.

The clear disadvantages and dangers associated with DREs have not deterred state and county authorities from throwing themselves headlong into touchscreen technology. More than 40,000 machines made by Diebold alone are already in use in 37 states, and most are touchscreens. County after county is poised to spend hundreds of millions of dollars more on computer voting before next spring's presidential primaries. "They say

this is the direction they have to go in to have fair elections, but the rush to go towards computerisation is very dubious," Dr Mercuri says. "One has to wonder why this is going on, because the way it is set up it takes away the checks and balances we have in a democratic society. That's the whole point of paper trails and recounts."

Anyone who has struggled with an interactive display in a museum knows how dodgy touchscreens can be. If they don't freeze, they easily become misaligned, which means they can record the wrong data. In Dallas, during early voting before last November's election, people found that no matter how often they tried to press a Democrat button, the Republican candidate's name would light up. After a court hearing, Diebold agreed to take down 18 machines with apparent misalignment problems. "And those were the ones where you could visually spot a problem," Dr Mercuri says. "What about what you don't see? Just because your vote shows up on the screen for the Democrats, how do you know it is registering inside the machine for the Democrats?"

Other problems have shown up periodically: machines that register zero votes, or machines that indicate voters coming to the polling station but not voting, even when a single race with just two candidates was on the ballot. Dr Mercuri was part of a lawsuit in Palm Beach County in which she and other plaintiffs tried to have a suspect Sequoia machine examined, only to run up against the brick wall of the trade-secret agreement. "It makes it really hard to show their product has been tampered with," she says, "if it's a felony to inspect it."

As for the possibilities of foul play, Dr Mercuri says they are virtually limitless. "There are literally hundreds of ways to do this," she says. "There are hundreds of ways to embed a rogue series of commands into the code and nobody would ever know because the nature of programming is so complex. The numbers would all tally perfectly." Tampering with an election could be something as simple as a "denial-of-service" attack, in which the machines simply stop working for an extended period, deterring voters faced with the prospect of long lines. Or it could be done with invasive computer codes known in the trade by such nicknames as "Trojan horses" or "Easter eggs". Detecting one of these, Dr Mercuri says, would be almost impossible unless the investigator knew in advance it was there and how to trigger it. Computer researcher Theresa Hommel, who is alarmed by touchscreen systems, has constructed a simulated voting machine in which the same candidate always wins, no matter what data you put in. She calls her model the Fraud-o-matic, and it is available online at www.wheresthepaper.org.

It is not just touchscreens which are at risk from error or malicious intrusion. Any computer system used to tabulate votes is vulnerable. An optical scan of ballots in Scurry County, Texas, last November erroneously declared a landslide victory for the Republican candidate for county commissioner; a subsequent hand recount showed that the Democrat had in fact won. In Comal County, Texas, a computerised optical scan found that three different candidates had won their races with exactly 18,181 votes. There was no recount or investigation, even though the coincidence, with those recurring 1s and 8s, looked highly suspicious. In heavily Democrat Broward County, Florida—which had switched to touchscreens in the wake of the hanging chad furore—more than 100,000 votes were found to have gone "missing" on election day. The votes were reinstated, but the glitch was not adequately explained. One local official blamed it on a "minor software thing".

Most suspect of all was the governor's race in Alabama, where the incumbent Democrat, Don Siegelman, was initially declared the winner. Sometime after midnight, when polling station observers and most staff had gone home, the probate judge responsible for elections in rural Baldwin County suddenly "discovered" that Mr Siegelman had been awarded 7,000 votes too many. In a tight election, the change was enough to hand victory to his Republican challenger, Bob Riley. County officials talked vaguely of a computer tabulation error, or a lightning strike messing up the machines, but the real reason was never ascertained because the state's Republican attorney general refused to

authorise a recount or any independent ballot inspection.

According to an analysis by James Gundlach, a sociology professor at Auburn University in Alabama, the result in Baldwin County was full of wild deviations from the statistical norms established both by this and preceding elections. And he adds: "There is simply no way that electronic vote counting can produce two sets of results without someone using computer programmes in ways that were not intended. In other words, the fact that two sets of results were reported is sufficient evidence in and of itself that the vote tabulation process was compromised." Although talk of voting fraud quickly subsided, Alabama has now amended its election laws to make recounts mandatory in close races.

The possibility of flaws in the electoral process is not something that gets discussed much in the United States. The attitude seems to be: we are the greatest democracy in the world, so the system must be fair. That has certainly been the prevailing view in Georgia, where even leading Democrats—their prestige on the line for introducing touchscreen voting in the first place—have fought tooth-and-nail to defend the integrity of the system. In a phone interview, the head of the Georgia Technology Authority who brought Diebold machines to the state, Larry Singer, blamed the growing chorus of criticism on "fear of technology", despite the fact that many prominent critics are themselves computer scientists. He says: "Are these machines flawless? No. Would you have more confidence if they were completely flawless? Yes. Is there such a thing as a flawless system? No." Mr Singer, who left the GTA straight after the election and took a 50 per cent pay cut to work for Sun Microsystems, insists that voters are more likely to have their credit card information stolen by a busboy in a restaurant than to have their vote compromised by touchscreen technology.

Voting machines are sold in the United States in much the same way as other government contracts: through intensive lobbying, wining and dining. At a recent national conference of clerks, election officials and treasurers in Denver, attendees were treated to black-tie dinners and other perks, including free expensive briefcases stamped with Sequoia's company logo alongside the association's own symbol. Nobody in power seems to find this worrying, any more than they worried when Sequoia's southern regional sales manager, Phil Foster, was indicted in Louisiana a couple of years ago for "conspiracy to commit money laundering and malfeasance". The charges were dropped in exchange for his testimony against Louisiana's state commissioner of elections. Similarly, last year, the Arkansas secretary of state, Bill McCuen, pleaded guilty to taking bribes and kickbacks involving a precursor company to ES&S; the voting machine company executive who testified against him in exchange for immunity is now an ES&S vice-president.

If much of the worry about vote-tampering is directed at the Republicans, it is largely because the big three touchscreen companies are all big Republican donors, pouring hundreds of thousands of dollars into party coffers in the past few years. The ownership issue is, of course, compounded by the lack of transparency. Or, as Dr Mercuri puts it: "If the machines were independently verifiable, who would give a crap who owns them?" As it is, fears that US democracy is being hijacked by corporate interests are being fuelled by links between the big three and broader business interests, as well as extremist organisations. Two of the early backers of American Information Systems, a company later merged into ES&S, are also prominent supporters of the Chalcedon Foundation, an organisation that espouses theocratic governance according to a literal reading of the Bible and advocates capital punishment for blasphemy and homosexuality.

The chief executive of American Information Systems in the early Nineties was Chuck Hagel, who went on to run for elective office and became the first Republican in 24 years to be elected to the Senate from Nebraska, cheered on by the Omaha World-Herald newspaper which also happens to be a big investor in ES&S. In yet another clamorous conflict of interest, 80 per cent of Mr Hagel's winning votes—both in 1996 and again in 2002—were counted, under the usual terms of confidentiality, by his own

company.

In theory, the federal government should be monitoring the transition to computer technology and rooting out abuses. Under the Help America Vote Act, the Bush administration is supposed to establish a sizeable oversight committee, headed by two Democrats and two Republicans, as well as a technical panel to determine standards for new voting machinery. The four commission heads were supposed to have been in place by last February, but so far just one has been appointed. The technical panel also remains unconstituted, even though the new machines it is supposed to vet are already being sold in large quantities—a state of affairs Dr Mercuri denounces as "an abomination".

One of the conditions states have to fulfil to receive federal funding for the new voting machines, meanwhile, is a consolidation of voter rolls at state rather than county level. This provision sends a chill down the spine of anyone who has studied how Florida consolidated its own voter rolls just before the 2000 election, purging the names of tens of thousands of eligible voters, most of them African Americans and most of them Democrats, through misuse of an erroneous list of convicted felons commissioned by Katherine Harris, the secretary of state doubling as George Bush's Florida campaign manager. Despite a volley of lawsuits, the incorrect list was still in operation in last November's mid-terms, raising all sorts of questions about what other states might now do with their own voter rolls. It is not that the Act's consolidation provision is in itself evidence of a conspiracy to throw elections, but it does leave open that possibility.

Meanwhile, the administration has been pushing new voting technology of its own to help overseas citizens and military personnel, both natural Republican Party constituencies, to vote more easily over the internet. Internet voting is notoriously insecure and open to abuse by just about anyone with rudimentary hacking skills; just last January, an experiment in internet voting in Toronto was scuppered by a Slammer worm attack. Undeterred, the administration has gone ahead with its so-called SERVE project for overseas voting, via a private consortium made up of major defence contractors and a Saudi investment group. The contract for overseeing internet voting in the 2004 presidential election was recently awarded to Accenture, formerly part of the Arthur Andersen group (whose accountancy branch, a major campaign contributor to President Bush, imploded as a result of the Enron bankruptcy scandal).

Not everyone in the United States has fallen under the spell of the big computer voting companies, and there are signs of growing wariness. Oregon decided even before HAVA to conduct all its voting by mail. Wisconsin has decided it wants nothing to do with touchscreen machines without a verifiable paper trail, and New York is considering a similar injunction, at least for its state assembly races. In California, a Stanford computer science professor called David Dill is screaming from the rooftops on the need for a paper trail in his state, so far without result. And a New Jersey Congressman called Rush Holt has introduced a bill in the House of Representatives, the Voter Confidence and Increased Accessibility Act, asking for much the same thing. Not everyone is heeding the warnings, though. In Ohio, publication of the letter from Diebold's chief executive promising to deliver the state to President Bush in 2004 has not deterred the secretary of state—a Republican—from putting Diebold on a list of preferred voting-machine vendors. Similarly, in Maryland, officials have not taken the recent state-sponsored study identifying hundreds of flaws in the Diebold software as any reason to change their plans to use Diebold machines in March's presidential primary.

The question is whether the country will come to its senses before elections start getting distorted or tampered with on such a scale that the system becomes unmanageable. The sheer volume of money offered under HAVA is unlikely to be forthcoming again in a hurry, so if things aren't done right now it is doubtful the system can be fixed again for a long time. "This is frightening, really frightening," says Dr Mercuri, and a growing number of reasonable people are starting to agree with her. One such is John Zogby,

arguably the most reliable pollster in the United States, who has freely admitted he "blew" last November's elections and does not exclude the possibility that foul play was one of the factors knocking his calculations off course. "We're ploughing into a brave new world here," he says, "where there are so many variables aside from out-and-out corruption that can change elections, especially in situations where the races are close. We have machines that break down, or are tampered with, or are simply misunderstood. It's a cause for great concern."

Roxanne Jekot, who has put much of her professional and personal life on hold to work on the issue full time, puts it even more strongly. "Corporate America is very close to running this country. The only thing that is stopping them from taking total control are the pesky voters. That's why there's such a drive to control the vote. What we're seeing is the corporatisation of the last shred of democracy.

"I feel that unless we stop it here and stop it now," she says, "my kids won't grow up to have a right to vote at all."