

# Electronic Voting: America's Vote at Risk

What You Need to Know,  
and What You Can Do About It

*"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.  
[We wonder] if democracy in America can survive."*

- [The Independent, October 14, 2003](#) -

Prepared for:

The House Committee on Administration,  
The Election Assistance Commission,  
The Media,  
but especially for

*The Citizens of the United States*

By:

Lisa Pease  
Los Angeles, California  
March, 2004

## Table of Contents

Introduction .....	3
How We Got Here - In Brief .....	4
Problems with Electronic Voting .....	5
Races REVERSED on an Electronic Error .....	5
Races with Strange Results.....	6
The Issue of Reliability .....	6
The Big Question - <i>How Would We Know?</i> .....	7
The Question of Ownership.....	8
Partisan Owners.....	8
Diebold .....	8
Election Systems & Services (ES&S) .....	8
Sequoia Voting Systems .....	9
Hart Intercivic.....	9
Solutions .....	10
We Need a Federal Solution .....	10
The Bills That Offer What We Need NOW .....	10
HR 2239 - Rush Holt's Bill.....	10
SB 1980 - Senate version of Rush Holt's Bill .....	11
What You Must Do.....	11
Appendix A: Experts on Electronic Voting Who Must Testify in Open Hearings .....	12
Beverly Harris.....	12
Professor David Dill .....	12
Rebecca Mercuri, Ph.D. ....	12
Avi Rubin .....	13
Appendix B: Voting Errors - Partial Summary Listing .....	14
Appendix C: Foreign Perspectives on E-Voting in America .....	23
<i>The New Zealand Herald</i> , October 19, 2003 .....	23
<i>The Independent (London)</i> , October 14, 2003 .....	26
Appendix D: The Last Word - Paul Krugman, <i>NYT</i> .....	35

## INTRODUCTION

**Who am I and why should you care?** I have served on the paid staffs of two separate Presidential campaign efforts (most recently for Howard Dean, and in 1992 for Jerry Brown's effort). I am a published editor, author, and researcher on governmental and corporate misdeeds (see *The Assassinations*, published by Feral House in Los Angeles, 2003). I am also a computer professional (formerly of Microsoft) who has created and managed public and private electronic databases. **This combination makes me uniquely qualified** to comment on how a purely electronic voting system has the potential to destroy the integrity of our vote and consequently, the legitimacy of our government.

**The legitimacy of any government depends on the informed consent of the governed.** I've spent years battling the "informed" part as the media becomes more a form of entertainment and an outlet for official propaganda than a source for citizens to educate themselves on the issues of the day. **With the advent of electronic voting, it's clear that now the voter's "consent" is at risk.**

**This document outlines:**

- The core issues that pose a threat
- The people that the new Election Assistance Commission needs to schedule for its upcoming public hearings
- The bills before the US House and Senate that need to be passed to protect the rights of all Americans to ensure a fair and accurate vote.

**There is a large, activist base of people** connected across the Internet who are committed to doing whatever it takes to see that our vote is protected. **This is an issue on the brink of the "tipping point."** The time to act is now.

***We have only one chance to get this right,*** because if we get it wrong, we may never have the ability to vote out the people who allowed this to happen or to vote in the people who could fix this.

## HOW WE GOT HERE - IN BRIEF

**How did we get to this point?** In the wake of the debacle of the 2000 Presidential election, which brought us new terms like “pregnant chad” and “butterfly ballots” we all saw that our election systems were not working on many levels. There were overvotes and undervotes. People had been scrubbed from voter rolls simply because they had the same name as a convicted felon. Ballots from overseas were allowed even though there was no postmark to indicate the date or even the point of original. There were a host of problems that came out, and a commission was formed to investigate the matter. The result of the investigations was the “[Help America Vote Act](#)”, commonly known as HAVA.

HAVA has broad and important requirements that are useful and helpful, like making it mandatory for states to keep clean and accurate voter rolls so people who should be able to vote can and those who shouldn't be able to vote cannot. HAVA also stresses the importance of providing a means for the blind to be able to cast a vote. In an effort to promote comprehensive voting reform, HAVA mandated that all 50 states have in place a voting system that meets certain requirements. In addition, HAVA offers states compensation for implementing new systems that meet these requirements. **Specifically, HAVA requires at least one machine in each polling place to be an electronic voting machine, and offers money to states to help them adopt such technology.** The clear message in HAVA, and the way that states are interpreting it, is that electronic voting should be implemented across all states as quickly as possible.

*In theory, and I stress in theory only,* electronic voting *is* the easiest way to meet the HAVA requirements. **In a perfect world,** where everyone wrote bug-free code and no one ever committed election fraud, this would make sense and would be the cheapest, most cost-effective way to hold a vote. **But let's talk reality.** I've worked at a major software company. Even the best programmers make serious mistakes. And ballot box stuffing, lever manipulation and other techniques to illegally obtain or deny votes have been with us from the dawn of voting and will be with us until this planet is no longer inhabitable. To assume that because something can be done by technology means it will suddenly become honest shows an incredible naïveté about the realities of politics. Paper can be altered, but it takes many people in many places to do this. **ONE database administrator** with the appropriate level of access can change an entire database in an undetectable way that **can reverse elections results. And no one would ever know.**

## PROBLEMS WITH ELECTRONIC VOTING

**Any computer professional will tell you that you can't entirely trust a machine programmed by a human being.** Errors are all too common. And worse, hackers are ever-present. Witness the number of viruses you've been sent in e-mail over the last year. Add to this mix that the outcome of an election can affect the spending of billions of dollars, and you have a strong profit incentive for some to manipulate a vote.

**In this section I am only *touching* on the issues.** A great wealth of in-depth reporting has already occurred on this subject. Many articles on voting mishaps can be found via a search of Google on the Internet, or any of the news service databases.

The **most commonly repeated misinformation** is that **no error has yet affected the outcome of an actual election.** As the data below will show, **this is provably not true.**

### Races REVERSED on an Electronic Error

Bear in mind that these are only the problems that were caught and checked, which led to reversals of the election. How many other cases have sailed by, unchallenged? *In reality, we have no way to prove that a race wasn't tampered with.*

Here are three straightforward examples where a race was reversed due to electronic issues:

- "The discovery of **a computer glitch reversed one outcome from this month's primary elections in Kansas**, and an unsuccessful candidate in another race has based his request for a special election on technical difficulties that allegedly occurred in his race. In Clay County, **computer results...had challenger Roy Jennings defeating incumbent Jerry Mayo by 22 votes. The hand recount...revealed Mayo as the winner and by a landslide, 540 votes to 175.**" ([Associated Press story / Lawrence Journal World, 8/22/02](#))
- In Alabama's Baldwin County, Don Siegelman had been awarded an election over Republican Bob Riley. But as it turned out, "Siegelman had actually only received 12,736 votes--not the 19,070 the Associated Press projected for him. A computer glitch had caused the error. **The erroneous tally would have put Siegelman on top by 3,582 votes, but the corrected one gave Riley a 2,752-vote edge.**" ([The Weekly Standard, 11/25/02](#))
- In Scurry County, Texas, in the November 2002 election, "**A defective computer chip** in the county's optical scanner misread ballots Tuesday night and **incorrectly tallied a landslide victory for Republicans. Democrats actually won by wide margins.** The problem was discovered when **poll workers became suspicious of the margins of the vote....**"

There are *many* other such examples. Beverly Harris's book *Black Box Voting: Ballot Tampering in the 21st Century* is an excellent place to start. You can read this book for free, online at [www.blackboxvoting.org](http://www.blackboxvoting.org). A great deal of data concerning overturned elections can be found in Chapter 2.

## Races with Strange Results

Even where a race was not reversed, there is serious cause for concern. If the truth had been discernable, perhaps these results would have been overturned as well.

- In Colmal County, Texas, **three Republicans got exactly the same number of votes**, while the Democratic challengers got different numbers of losing results. (*La Prensa de San Antonio*, 1/18/2004)
- "After recounting more than 13,000 absentee paper ballots, Northern California's Napa County reported Thursday that **an electronic voting machine** used in the March 2 primary election **missed more than 6,000 votes**. The recount did not change the outcome of any races, but a spokesman for a state legislator said the glitch highlighted the need for using only e-voting machines that produce a paper trail." ([Wired News](#), 3/19/04)
- In Alameda and San Diego Counties, California, "**large-scale failure of electronic devices** used to produce ballot-access cards for voters -- **delayed Super Tuesday voting at 200 polling places** in Alameda County and more than 560 in San Diego County. When paper ballots ran out, hundreds of voters were turned away. ...

"For the first time, Clark's letter suggests **Alameda County also had unspecified "programming problems" in the Democratic and American Independent Party presidential primaries**. ... Clark also made note of "absentee ballot problems," a reference to a glitch in the Oct. 7 recall election that **mysteriously awarded thousands of absentee votes for Democratic Lt. Gov. Cruz Bustamante to Southern California Socialist John Burton**. A Diebold technician changed the votes based on examination of the paper ballots and scanned ballot images.

"**"I am sure that it was fixed because of the hand counts that we did,"** Clark said in a recent e-mail, "**but I was not satisfied with the answers as to why it happened.**" ([Alameda Times Star](#), 3/24/04)

The only way errors have *ever* been detected was through a challenge and through a check of *some other system, usually a manual count of some sort*. Without that, we have no way to audit results.

## The Issue of Reliability

As the quotes below show, we really shouldn't be trusting our most precious right, our right to vote, to trust to these machines and their programmers.

- "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 Massachusetts 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 Independent](#), 10/14/03)

- "My research team observed that the encryption of the modem connection was carried out incorrectly in the Diebold machines so that **anyone able to tap the phone lines would be able to tamper with the tally and change votes**. In my precinct, the phone line didn't work; the memory cards were taken to the Board of Elections office by the chief judges." — Avi Rubin, in an editorial to the [Oakland Tribune 3/12/04](#), commenting on his first-hand experience as an election judge in Alameda County, CA.
- "I think it's fair to say from the evidence so far that **the test flight crashed and burned**." — State Senator Don Perata (Oakland, CA Democrat in the wake of the March 2, 2004 CA primary, using electronic voting machines), *Los Angeles Times*, March 12, 2004.

**In brief, already demonstrated problems with electronic voting come from:**

- unreliable code (whether deliberate or accidental)
- unreliable hardware from the machine manufacturers
- lack of training of the polling place staff
- vulnerability to power outages
- vulnerability of modem access to get votes to HQ for roll-up tallying
- vulnerability of [wireless access](#) to get votes to HQ (wireless is inherently insecure, as is a modem line)
- no voter-verified paper ballot for auditing
- no automatic hand-recount procedure in place, whether in close elections or not. Some problems have occurred in elections that were not deemed close, so we cannot rely upon recounts called for in close elections.

Again, for further detail, please do your own reading. This is merely a short summary.

## **The Big Question - *How Would We Know?***

The obvious question to ask, which cannot be answered, is in how many races would the results have gone another way had a manual recount taken place?

And without paper records of the votes, how could there be any audit at all? And even with paper, if it's not voter-verified, what's the point?

How dare we trust our most precious public right, the right to elect our own representation, to a black box system?

## THE QUESTION OF OWNERSHIP

*"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."*

— *The New Zealand Herald* (10/19/03), quoting American Roxanne Jekot

### Partisan Owners

There are four major players who already control a great portion of the electronic voting market. These are:

- Diebold (of North Canton, OH)
- Election Systems & Services (ES&S, of Omaha, Nebraska)
- Sequoia Voting Systems, Inc. (of Oakland, CA)
- Hart Intercivic (of Austin, TX)

Examine these companies briefly. The data for these companies is summarized from the April 2004 issue of *Vanity Fair*.

#### DIEBOLD

Diebold's president Wally O'Dell has become famous for his public remark that he would do all he could to ensure that Ohio's electoral votes are delivered to Bush in 2004. Naturally, Wally doesn't want people thinking he'll have Diebold give away the election. But given their track record, this isn't a far-fetched fantasy. Max Clelland, the Democratic incumbent Senator in Georgia, lost to a rival Republican newcomer in the 2002 Georgia election. Clelland had been well ahead in all the polls just two days before the election - yet lost by a swing in 12 percent of the vote. Some point to Republican ads that persuaded the voters. But others say that Diebold was to blame. Diebold's files couldn't have made them look more suspicious. When Beverly Harris stumbled upon an FTP site of Diebold's election program files, one suspicious folder was named "rob-georgia".

#### ELECTION SYSTEMS & SERVICES (ES&S)

Election Systems & Services (formerly Data Mark Systems and American Information Systems) was founded by Todd and Bob Urosevich. Today, Todd is Vice President of Customer Support for ES&S. Bob, however, is now the President of Diebold. So we have the appearance, but not necessarily the reality, of competition among the vendors. ES&S's history bears a heavy Republican presence.

ES&S has a bit of a sordid history. Former Nebraska Senator Chuck Hagel was both an investor of and a beneficiary of this company, as ES&S was used when he won his surprise

election to the Senate in 1996. He claimed to have ended his involvement with ES&S in 1995, but in reality held shares in the McCarthy Group, which owned the company that became ES&S. In addition, Hagel's campaign treasurer, Michael McCarthy, was the McCarthy in the "McCarthy Group". These sorts of conflicts of interests should not be allowed so close to our vote.

ES&S is into the scratch-my-back-I'll-scratch-yours game that lobbyists in Washington know all to well. Do business with us today and we'll give you a job tomorrow. ES&S has done exactly that - hiring former secretaries of state from Florida and California after those same people held positions that required them to recommend an electronic voting vendor.

### **SEQUOIA VOTING SYSTEMS**

Sequoia has as sordid a history as Diebold and ES&S, if not worse. Sequoia's salesman Phil Foster had been delivering envelopes filled with large bundles of cash on five occasions to an intermediary enroute to Louisiana elections commissioner Jerry Fowler. Foster denies he knew he was delivering cash, but can his denial be believed? Especially when it turns out his brother-in-law J. David Philpot was the one giving him the cash to deliver? Does it matter that Philpot's scam was to sell his own election machines under the cover of Sequoia, but not Sequoia's machines? Does it make you feel better to know that Sequoia isn't even owned by an American company, but by a British corporation? Do we want to entrust our vote to foreign owners? And does it help to know that ES&S and Sequoia have done joint lobbying efforts to push electronic voting, and have shared personnel?

### **HART INTERCIVIC**

Hart Intercivic has a Republican angel as well — Texas investor Tom Hicks of Stratford Capital Partners. Hicks was instrumental in the purchase of the Texas Rangers from George W. Bush in 1998, giving him a \$14.9 million cash infusion which surely helped his 2000 presidential bid. Hicks has given over \$125,000 to the Republicans since 1999, and invests heavily in Clear Channel, the company famous for airing right-wing radio across the land and for censoring the Dixie Chicks when they criticized the President over the Iraq war.

**In summary, should we trust our vote to partisan-owned and financed firms? Should we allow so much interbreeding between these few companies? Shouldn't our vote be free from the possible influence of zealots and "true believers"?**

## SOLUTIONS

The best minds on this subject have spoken out consistently on these common principles:

- Electronic should never be allowed unless there is a paper record to back up the electronic record.
- A paper record should only be considered valid if the voter personally verified its accuracy.
- Having a voter-verified paper record means nothing if that record is never audited in a recount.
- Waiting for a recount to be requested means handing most elections to the electronic victor, whether or not the count was accurate.

In other words, what we really need is this:

- An Electronic vote with a voter-verified paper backup record.
- A mandatory, surprise, statistically significant hand recount of the voter-verified paper ballot in all elections.

Normally, to challenge a vote, a candidate has to request a recount, and then the burden of the cost of the recount falls to the challenger. If the recount proves that the requestor won, then the requestor does not have to pay. But if the requestor loses the recount, the requestor pays the recount cost. This makes asking for a recount prohibitively expensive for a candidate, which is why so few take place. We need to ensure a *mandatory, surprise* recount. In other words, we can't say in advance which precincts will be recounted. That would defeat the purpose of the audit.

Only if all these conditions are met can the public have *any* confidence whatsoever in the veracity of the vote, and therefore the legitimacy of the government.

## We Need a Federal Solution

There isn't time to get this data out state by state. Our vote is in peril *now*, and protecting the legitimacy of the Republic requires a federal solution. If we had seen this coming, we could have fought this state-by-state. Now, it's just too late. We need a federal law to protect our elections.

## The Bills That Offer What We Need NOW

### HR 2239 - RUSH HOLT'S BILL

This bill has what is needed to protect our vote. You can read the entire bill, monitor co-sponsors and track bill activity at [thomas.loc.gov](http://thomas.loc.gov). Thomas is a system of the Library of Congress that provides citizens access to pending legislation.

Currently, Holt's bill has been stifled in the Committee on House Administration, which Republicans control. For the credibility of our government, this bill must come to a vote.

## **SB 1980 - SENATE VERSION OF RUSH HOLT'S BILL**

If and when Holt's bill passes the House, a duplicate bill awaits in the Senate. Again, you can monitor the status and progress of this bill at the Thomas site above.

There are competing bills in the Senate. Remember that having a paper record, even a voter-verified record, is useless without the *mandatory* surprise percentage recount. SB 1980 guarantees this. One of the competing Senate bills only *recommends* this. That's a huge difference. Stick with Holt's language, replicated in SB 1980 (introduced by former Florida Governor and current Florida Senator Bob Graham. He's done the best work in Congress on this case so far.

## **What You Must Do**

- **Tell your friends about the extreme vulnerability of your vote.** Impress upon them the urgency of this issue. After November, 2004, we may not have this chance again.
- **Press your Congressperson an**

## APPENDIX A: EXPERTS ON ELECTRONIC VOTING WHO MUST TESTIFY IN OPEN HEARINGS

One of the requirements of HAVA was to create an Election Assistance Commission. This Commission is then charged with coming up with a report, and is calling people to testify before the commission in a series of public hearings starting (presumably) in April, 2004.

The following people have devoted months and in a couple of cases, years to the research of electronic voting. All have important, well-detailed lists of issues, potential issues, and proposed solutions. These people *must* be asked to testify at public hearings if the hearings are to have any credibility with those with even a passing familiarity with this issue.

### Beverly Harris

Author of Black Box Voting

[www.blackboxvoting.com](http://www.blackboxvoting.com) and [www.blackboxvoting.org/](http://www.blackboxvoting.org/)

Beverly Harris is, without a doubt, *the* leading authority on the question of ownership of the machines. She should be asked to testify about the people who own and run these machines.

330 SW 43rd St

PMB K-547

Renton WA 98055

Phone: 425-228-7131

Fax: 425-228-3965

e-mail: [feedback@talion.com](mailto:feedback@talion.com)

### Professor David Dill

Professor of Computer Science at Stanford University

[www.verifiedvoting.org](http://www.verifiedvoting.org)

Researcher in "formal verification" for 20 years; has served on several vote-related state and county task forces

Department of Computer Science

Gates Building 3A

Stanford, CA 94305-9030

Phone: (650) 725-3642

Fax: (650) 725-6949

E-mail: [dill@cs.stanford.edu](mailto:dill@cs.stanford.edu)

### Rebecca Mercuri, Ph.D.

Rebecca Mercuri earned her doctorate with a thesis entitled "Electronic Vote Tabulation: Checks and Balances" at the University of Pennsylvania. She has testified before numerous bodies regarding electronic voting.

[www.notablessoftware.com/evote.html](http://www.notablessoftware.com/evote.html)

P.O. Box 1166 -- Dept. EV  
Philadelphia, PA 19105  
Phone: 609/895-1375 or 215/327-7105  
E-mail: [mercuri@acm.org](mailto:mercuri@acm.org)

## **Avi Rubin**

Avi Rubin is a computer science professor at Johns Hopkins University and has been an election judge, as well as a leader on this issue.

[avirubin.com](http://avirubin.com)

JHUISI

3100 Wyman Park Drive  
Wyman Park Bldg. 4th Floor  
Baltimore, MD 21211

Phone: (410) 516-8177

Fax: (413) 208-9184

E-mail: [rubin@jhu.edu](mailto:rubin@jhu.edu) (Work)  
[avi@rubin.net](mailto:avi@rubin.net) (Personal)

## APPENDIX B: VOTING ERRORS - PARTIAL SUMMARY LISTING

This is a short summary of some of the known problems with electronic voting machines in the last few years. This is not meant to be an all-inclusive list. In fact, it's not possible to list all problems because only those problems that were detected and reported made it into the public record. Imagine how many other problems never made it that far.

This list was prepared by:

Richard A. Stimson

High Point, NC ([stimso1@juno.com](mailto:stimso1@juno.com))

[North Carolina Coalition for Verifiable Voting](#)

Co-editor 158-page book "[Global Solutions](#)" - FREE

Author of other books at [www.stimson.homestead.com](http://www.stimson.homestead.com)

USA Coordinator, [International Simultaneous Policy Organisation](#)

### Alabama

**Date:** November 2002

**Area:** Baldwin County votes for Governor

**System:** ES&S

**Problem:** at close of polls the Democrat had won but next morning 6,300 of his votes had inexplicably disappeared making the Republican the winner - "Something happened. I don't have enough intelligence to say exactly what," said Mark Kelley of ES&S.

**Outcome:** recount requested and denied

**Source:** Mobile Register, Jan. 28, 2003, "Voting snafu answers elusive"

### California

**Date:** Nov. 2003

**Area:** Alameda County

**System:** Diebold Elections Systems Inc. touch-screen

**Problem:** Diebold altered the software running in touchscreen voting machines yet neither submitted it for state testing nor notified state authorities of the change

**Outcome:** Stanford computer science professor David L. Dill disputes state and county assurances that Diebold's recent software changes have no effect on election returns. "How are they going to prove it? They can't."

**Source:** Oakland Tribune

**Date:** Nov. 2003

**Area:** Riverside County

**System:** Sequoia Voting Systems; AVC Edge touch-screen system.

**Problem:** Software used for placing ballots on voting kiosks and for storing and tabulating results has been left unprotected on a publicly available server, by Jaguar Computer Systems, a firm that provides election support to a California county, raising concerns about the possibility of vote tampering in future elections.

**Outcome:** Jaguar blocked public access to the FTP site

**Source:** <http://www.wired.com/news/privacy/0,1848,61014,00.html>

## Florida

**Date:** March 2002

**Area:** Palm Beach County

**System:** Sequoia touch-screen machines

**Problem:** machines froze up when voter selected language

**Outcome:** Phil Foster of Sequoia said it was software programming error

**Source:** The Palm Beach Post, Mar. 14, 2002, "Human goofs, not machines..."

**Date:** Apr. 2002

**Area:** Medley town council election

**System:**

**Problem:** voting machines gave victory to wrong candidate

**Outcome:** elections supervisor concerned because computer didn't raise any red flags and humans had to spot the error

**Source:** Miami Herald, Apr. 4, 2002, "Despite new voting system..."

**Date:** Nov. 2002

**Area:** Broward County, Century Village precinct

**System:**

**Problem:** There were 7,515 votes in 1994, 10,947 in 1998, but only 4,179 in 2002 although population was stable after complex reach maximum occupancy in 1998

**Outcome:** suspicious but cause unknown

**Source:** Miami Herald, Nov. 10, 2002, and call-in from Miami accountant reported in "Black Box Voting" by Bev Harris

**Date:** April 2003

**Area:** Boca Raton (city council)

**System:** Sequoia touch-screen

**Problems:** (1) delayed count because of 15 lost cartridges said to have been taken home by poll worker, (2) voters choosing one candidate found check by another's name.

**Outcome:** independent computer experts not allowed to check machines

**Source:** Wyatt Olson; <http://www.newtimesbpb.com/issues/2003-04-24/feature.html/1/index.html>

## Georgia

**Date:** Nov. 2002

**Area:** Atlanta

**System:** touch-screen, no paper trail

**Problem:** memory cards for 67 machines misplaced and votes left out of total

**Outcome:** 56 memory cards found and recorded, 11 still unaccounted for

**Source:** Atlanta Constitution-Journal

**Date:** Nov. 2002

**Area:** County Commissioner

**System:** Optical scanner

**Problem:** "A defective computer chip in the county's optical scanner misread ballots Tuesday night and incorrectly tallied a landslide victory for Republicans...Democrats actually won by wide margins."

**Outcome:** error recognized and corrected by poll workers

**Source:** Associated Press, Nov. 7, 2002

## Indiana

**Date:** Nov. 4, 2003

**Area:** Boone County

**System:** MicroVote

**Problem:** Computer-generated vote totals showed 144,000 votes from 19,000 registered voters and a "computer glitch" was blamed

**Outcome:** collaboration between the county and advisers from the software producer was said to have fixed the problem

**Source:** Indianapolis Star, Nov. 9, 2003

## Kansas

**Date:** April 2002

**Area:** Johnson County

**System:** Diebold touch-screen

**Problem:** incorrect totals in six races, no paper trail

**Outcome:** recount from internal records changed results dramatically, Diebold tried to re-create the error in hope of correcting it, Diebold President Urosevich said "I wish I had an answer"

**Source:** investigative Journalist Bev Harris, author of the book "Black Box Voting: Ballot Tampering In The 21st Century "; also The Kansas City Star, Apr. 5, 2002, "Election errors unnerve Johnson County official"

**Date:** Aug. 2002

**Area:** Clay County, election of county commissioner

**System:**

**Problem:** machines said Mayo got 48% of vote, software programming errors

**Outcome:** hand count revealed Mayo got 76%

**Source:** AP report in Wichita Eagle, Aug. 22, 2002, "Mayo won by a landslide...election reversed..."

## Louisiana

**Date:** Nov. 2002

**Area:** St. Bernard Parish, Justice of the Peace election

**System:**

**Problem:** machine ate 35 absentee ballots

**Outcome:** even technician could not extract them from locked-up machine

**Source:** The Times-Picayune, Nov. 7, 2002, "Machine snag..."

**Date:** Nov. 2002

**Area:** Tangipahoa Parish

**System:**

**Problem:** 20% of machines malfunctioned according to clerk of court

**Outcome:** 15 of his employees worked to overcome malfunctions

**Source:** The Baton Rouge Advocate, Nov. 7, 2002, "Voting machine glitches..."

## Maryland

**Date:** 2002

**Area:** election for Governor, polling place in Croom

**System:** Diebold touch-screen

**Problem:** "I pushed a Republican ticket for Governor and his name disappeared...then the Democrat's name got an X put in it," Kevin West of Upper Marlboro reported.

**Outcome:** no one will ever know because system is unauditible

**Source:** The Washington Times, Nov. 6, 2002, "Glitches cited at some polls..."

**Date:** 2002

**Area:**

**System:** Diebold touch-screen

**Problem:** many voters saw a banner announcing "Democrat" at the top of their screen regardless of their choice

**Outcome:** no one will ever know how those votes were recorded

**Source:** The Washington Times, Nov. 6, 2002, "Glitches cited at some polls..."

**Date:** Aug. 12, 2003

**Area:** statewide

**System:** Diebold touch-screen

**Problem:** a study by three researchers from the Johns Hopkins Information Security Institute and a computer scientist at Rice University analyzed programming code and concluded the system was vulnerable to unscrupulous voters, as well as "insiders such as poll workers, software developers and even janitors," who could cast multiple votes without a trace

**Outcome:** Maryland expanded the use of these machines from four counties to the entire state – another company was contracted to audit the system under a non-disclosure agreement

**Source:** Brian Witte, ASSOCIATED PRESS  
and <http://www.wired.com/news/technology/0,1282,59976,00.html>

## Nebraska

**Date:** 1996 and 2002

**Area:** statewide 85% of votes cast in Senate election

System: ES&S

**Problem:** Sen. Chuck Hagel, former talk show host had his votes counted by the company he headed until March 1995 and in whose parent company, headed by Hagel's campaign manager, he owns part interest

**Outcome:** Hagel declined to disclose to the Senate Ethics Committee the value of assets he held in the parent company based on a technicality

**Source:** Washington, D.C., publication "The Hill", Jan.3, 2003  
(<http://www.thehill.com/news/012903/hagel.aspx>)

**Date:** Nov. 2002

**Area:** Gretna

System: ES&S

**Problem:** machines failed to tally "yes" votes on school bond issue

**Outcome:** bond issue actually passed by a 2-1 ratio

**Source:** Omaha World Herald, Nov. 6, 2002, "A late night in Sarpy..."

**Date:** Nov. 2002

**Area:** U.S. Senate race

**System:** optical scan

**Problem:** Democratic candidate found his ballot had already been filled out for his opponent, Chuck Hagel

Outcome:

**Source:** Interview with Charlie Matulka, Dem. Candidate reported in "Black Box Voting" by Bev Harris

## New Jersey

**Date:** Nov. 2002

**Area:** Cherry Hill

System:

**Problem:** 96% of machines couldn't register votes for mayor, despite pretesting and certification

**Outcome:** up to 100 early voters turned away from the polls

**Source:** Newsweek, Nov. 6, 2003, "Voting glitches..."

**Date:** Nov. 2002

**Area:** Mays Landing County

System:

**Problem:** computer "irregularity" caused 3 of 5 relay stations to fail

**Outcome:** county clerk was given something resembling cash register tapes for a hand count

**Source:** Newsweek, Nov. 6, 2003, "Voting glitches..."

## New Mexico

**Date:** Nov. 2002

**Area:** Taos

**System:** optical scanner

**Problem:** county clerk noticed computer was counting votes under wrong name

**Outcome:** programmer told her it was a programming error

**Source:** Albuquerque Journal, Nov. 7, 2002, "Taos to recount absentee ballots"

## New York

**Date:** Nov. 2002

**Area:** Monroe County

**System:**

**Problem:** programming errors confused vote tally and election officials pulled the plug on the vote-reporting website

**Outcome:** voting machine tallies were impounded and guarded overnight by a deputy sheriff

**Source:** Rochester Democrat & Chronicle, Nov. 7, 2002, "John squeaks out victory..."

## North Carolina

**Date:** Oct.-Nov., 2002

**Area:** Wake County

**System:** Election Systems and Software: touch-screen equipment, called iVotronic machines

**Problem:** in early voting 294 of 2,228 ballots cast on the malfunctioning machines were not recorded, many voters tried to record their choices two, three or four times before it would register

**Outcome:** elections officials would try to reach everyone in time to let them vote again

**Source:** Raleigh News & Observer, by J. Andrew Curliss

**Date:** Nov. 2002

**Area:** Wayne County, House District 11

**System:**

**Problem:** mistake in computer programming caused vote-counting machines to skip thousands of straight tickets of both major parties

**Outcome:** finding 5,500 more votes reversed the election of state representative

**Source:** The News & Observer, Nov. 9, 2002, "'Winners' may be losers"

## Ohio

**Date:** Nov. 2002

**Area:** Crawford County

System:

**Problem:** 2 vote counting machines failed

**Outcome:** workers drove to another county to borrow the use of a machine

**Source:** Telegraph-Forum, Nov. 6, 2002, "Glitch sends vote count to Richland"

## Pennsylvania

**Date:** May 2001

**Area:** Pittsburgh's 12th and 13th wards

System:

**Problem:** councilwoman reported that machines in these and other predominantly black neighborhoods began smoking and spitting out crumpled paper

**Outcome:** repairs took hours and voters who couldn't wait that long lost their vote

**Source:** Pittsburgh Post-Gazette, May 4, 2001, "Hearing Gets Landslide of Voting Problems"

## South Carolina

**Date:** Nov. 2002

**Area:** Pickens County

System:

**Problem:** unable to get totals from two precincts because of computer glitches

Outcome:

**Source:** Associated Press, Nov. 6, 2002

**Date:** Nov. 2002

**Area:** race for state commissioner of agriculture

System:

**Problem:** 21,000 votes uncounted (55%)

**Outcome:** fortunately there were paper ballots for a hand count

**Source:** The Herald, Rock Hill, SC, Nov. 7, 2002, "Machine glitch keeps votes from being counted"

## Texas

**Date:** Nov. 2002

**Area:** Dallas

System:

**Problem:** 18 machines found to register Republican when voters pushed Democrat were taken out of action

**Outcome:** Republican judge quashed effort to investigate accuracy of the tally

**Source:** Fort Worth Star-Telegram, Oct. 30, 2002, "Democrats to appeal..."

**Date:** 2002

**Area:** Comal County

**System:** touch-screen

**Problem:** three Republican candidates each won with exactly 18,181 votes, called weird

**Outcome:** no audit; according to County Clerk "just a big coincidence"

**Source:** Deseret News, Nov. 9, 2002, "Texans tally triple match..."; and "Lynching by Laptop" by Greg Palast and Ina Howard

**Date:** 2002

**Area:** Scurry County commissioner votes

**System:** optical scanner

**Problem:** "faulty" computer chip caused Democratic votes to be recorded as Republican and gave landslide wins to the wrong candidates

**Outcome:** two manual recounts and a replacement chip in the scanner confirmed the error and the original results were overturned

**Source:** Houston Chronicle, Nov. 8, 2002, "Ballot glitches reverse two election results"

## Virginia

**Date:** Nov. 2003

**Area:** Fairfax County (county offices)

**System:** WINvote computer technology from Advanced Voting Solutions of Frisco, Tex.

**Problem:** county officials tested one of the machines in question and discovered that it seemed to subtract a vote for a Republican candidate in about "one out of a hundred tries"; Republicans asked a Circuit Court judge to keep 10 voting machines under lock and key that broke down and were brought to the county government center for repairs and then returned to the polls – an alleged violation of election law.

**Outcome:** The judge said the activity logs of all 10 machines will be inspected this week, with members of both major parties present; county officials defended the system--"The new machines get an A-plus. It's the plan to collect the vote that gets the failing grade."

**Source:** David Cho, Washington Post Staff Writer, Thursday, November 6, 2003; Page B01

## Washington

**Date:** 2003

**Area:** King County

**System:** Diebold Election Systems

**Problem:** an internal Diebold e-mail, circulated last month on the Internet, said the county was "famous" for accessing the GEMS election database through a separate software program, Microsoft Access (not software that has been certified for election use)

**Outcome:** election director ordered the removal of Access and all other nonelection software from the main vote-tabulating computer and a backup computer

**Source:** Seattle Times, by Keith Ervin, staff reporter, Sun., Nov. 2, 2003

**Date:** Feb. 2003

**Area:** Everett, Snohomish County

**System:** Sequoia optical scan

**Problem:** 21.5% of ballots in 28 precincts were missed,

**Outcome:** Republicans asked for recount, 116,837 absentee ballots recounted

**Source:** Citizen meeting, Jan. 23, 2003, reported in "Black Box Voting" by Bev Harris



## APPENDIX C: FOREIGN PERSPECTIVES ON E-VOTING IN AMERICA

These two articles are stellar in outlining the perils of our new way of voting. They present excellent short summaries of key issues.

***The New Zealand Herald, October 19, 2003***

**Us Voting System Vulnerable To Fraud - Part 4**

*America's Vote At Risk*

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 introduci

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 voter rolls 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 who doubled 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 via the internet.

Internet voting is notoriously insecure and open to abuse by just about anyone with rudimentary hacking skills. 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 named 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, 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.

John Zogby, arguably the most reliable pollster in the United States, freely admits 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 said, "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."

## *The Independent (London), October 14, 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. Andrew Gumbel wonders if democracy in America can survive**

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 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 (pounds 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 debacle 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 (pounds 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 Massachusetts 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](http://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."

## APPENDIX D: THE LAST WORD - PAUL KRUGMAN, *NYT*

In the January 23, 2004 edition of *The New York Times* (p. A23), Paul Krugman wrote an excellent short summary of why we need to care. His column follows in full.

The disputed election of 2000 left a lasting scar on the nation's psyche. A recent Zogby poll found that even in red states, which voted for George W. Bush, 32 percent of the public believes that the election was stolen. In blue states, the fraction is 44 percent.

Now imagine this: in November the candidate trailing in the polls wins an upset victory -- but all of the districts where he does much better than expected use touch-screen voting machines. Meanwhile, leaked internal e-mail from the companies that make these machines suggests widespread error, and possibly fraud. What would this do to the nation?

Unfortunately, this story is completely plausible. (In fact, you can tell a similar story about some of the results in the 2002 midterm elections, especially in Georgia.) Fortune magazine rightly declared paperless voting the worst technology of 2003, but it's not just a bad technology -- it's a threat to the republic.

First of all, the technology has simply failed in several recent elections. In a special election in Broward County, Fla., 134 voters were disenfranchised because the electronic voting machines showed no votes, and there was no way to determine those voters' intent. (The election was decided by only 12 votes.) In Fairfax County, Va., electronic machines crashed repeatedly and balked at registering votes. In the 2002 primary, machines in several Florida districts reported no votes for governor.

And how many failures weren't caught? Internal e-mail from Diebold, the most prominent maker of electronic voting machines (though not those in the Florida and Virginia debacles), reveals that programmers were frantic over the system's unreliability. One reads, "I have been waiting for someone to give me an explanation as to why Precinct 216 gave Al Gore a minus 16022 when it was uploaded." Another reads, "For a demonstration I suggest you fake it."

Computer experts say that software at Diebold and other manufacturers is full of security flaws, which would easily allow an insider to rig an election. But the people at voting machine companies wouldn't do that, would they? Let's ask Jeffrey Dean, a programmer who was senior vice president of a voting machine company, Global Election Systems, before Diebold acquired it in 2002. Bev Harris, author of "Black Box Voting" ([www.blackboxvoting.com](http://www.blackboxvoting.com)), told The A.P. that Mr. Dean, before taking that job, spent time in a Washington correctional facility for stealing money and tampering with computer files.

Questionable programmers aside, even a cursory look at the behavior of the major voting machine companies reveals systematic flouting of the rules intended to ensure voting security. Software was modified without government oversight; machine components were replaced without being rechecked. And here's the crucial point: even if there are strong reasons to suspect that electronic machines miscounted votes, nothing can be done about it. There is no paper trail; there is nothing to recount.

So what should be done? Representative Rush Holt has introduced a bill calling for each machine to produce a paper record that the voter verifies. The paper record would then be secured for any future audit. The bill requires that such verified voting be ready in time for the 2004 election -- and that districts that can't meet the deadline use paper ballots instead. And it also requires surprise audits in each state.

I can't see any possible objection to this bill. Ignore the inevitable charges of "conspiracy theory." (Although some conspiracies are real: as yesterday's Boston Globe reports, "Republican staff members of the U.S. Senate Judiciary Committee infiltrated opposition computer files for a year, monitoring secret strategy memos and periodically

passing on copies to the media.") To support verified voting, you don't personally have to believe that voting machine manufacturers have tampered or will tamper with elections. How can anyone object to measures that will place the vote above suspicion?

What about the expense? Let's put it this way: we're spending at least \$150 billion to promote democracy in Iraq. That's about \$1,500 for each vote cast in the 2000 election. How can we balk at spending a small fraction of that sum to secure the credibility of democracy at home?