FOOLED AGAIN
STEAL THIS VOTE
THE CRISIS OF AMERICAN DEMOCRACY
was the 2004 presidential election stolen?
WHAT WENT WRONG IN OHIO

OUR DEMOCRACY AT RISK

Earning the right to vote has been a hard-fought struggle. Yet, the U.S. Census Bureau estimates that nearly one in three registered voters didn't vote in 2004 and more than 3.6 million votes went uncounted.

In addition to uncounted votes, there is a growing body of evidence indicating massive vote-switching -- and electronic voting machines are clearly implicated. Unintentionally or otherwise, these machines aren't counting our votes - or are counting them incorrectly.

As a result, only 45% of Americans believe that George W. Bush was elected "fair and square," according to a recent poll.

But electronic voting machines continue to proliferate. The U.S. Election Assistance Commission estimates that in November 2008, 95% of our votes will be cast on these machines. We ought to be asking election officials some tough questions:

Who's telling these machines what to do?

Voting machines—like all computers—do what they are told; and the public isn't allowed to know what they're being told to do by the manufacturers of voting systems that now control the casting and counting of our votes. Even election officials don't know what's going on inside these machines and have to rely on company technicians to keep them running on Election Day.

According to the voting machine companies, this software is "proprietary" and therefore can't be examined by voting officials or the public. Even reports from the testing labs (who are paid by vendors) are secret. By contrast, Las Vegas slot machine software is regularly inspected by the State of Nevada.

Are voting machines secure?

Smaller than a pack of cigarettes and less than half an inch thick - a touch-screen memory card holds thousands of votes - and it can spread computer viruses that change election results.

Electronic voting machines and systems are vulnerable to security breaches during manufacture and programming before they are purchased, while they are being serviced and stored, during Early Voting and on Election Day. Threats include:

- Corrupt or malicious software
- Remote wired or wireless attacks
- Attacks on the central tabulator

New York University Law School: A recent report by the Brennan Center for Justice identified more than 120 potential electronic voting system security threats.

Pennsylvania: Problems with Diebold touch-screens continued to surface in mid-2006: "It's the most severe security flaw ever discovered in a voting system," said Michael Shamos, the state's expert examiner.

Leon County, Florida: Computer engineer Harri Hursti hacked a test election on optical scan equipment in two minutes, without even a password. Any ordinary pollworker could do the same.

Princeton University: Researchers from the Center for Information Technology Policy released a study that showed it was possible to load malicious computer code into a touch-screen that would change an election without a trace and would spread like a virus, infecting other machines. They proved that a single individual can corrupt election results. See the video at:

www.ballot-integrity.org/video.htm

How reliable are these machines?

Due to poor design and quality control, voting machines are especially prone to start-up failures, screens freezing, loss of data, and other critical malfunctions. Failure rates of more than 10% are common.

Ascension Parish, LA - November, 2002
Voting System Vendor: ES&S
Over 200 of the ES&S machines (about 20%) malfunctioned on Election Day - overheating, locking up, and even shutting down while a voter was voting.

California: In volume testing by the Secretary of State in 2005, 34 of 96 Diebold TSx touch-screen machines (35.4%) failed due to software errors or printer jams. The test report concluded:

"It is hard to escape the conclusion that any system with failure rates this high is not ready for use in an election."

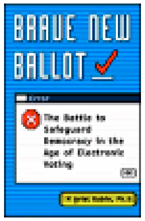
Can these machines count?

Ever since the use of electronic voting machines started to become widespread, hundreds of malfunctions and miscounts have been reported in state after state:

Volusia County, FL - November, 2000
Voting System Vendor: Global Election Systems
In one precinct a ***negative*** 16,022 votes were tallied for Al Gore, causing the race to be called for George W. Bush before the error was corrected.

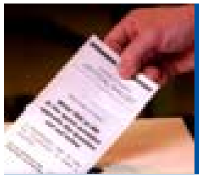
Bernalillo County, NM - November, 2004
Voting System Vendor: Sequoia
Certified tallies showed there were 2,087 more votes for president than there were voters who signed the pollbooks on election day.

Pottawattamie County, IA - May, 2006
Voting System Vendor: ES&S
A hand count revealed that every winner in the County's nine contested races had actually lost. The flawed results were due to a programming error.


BRAVE NEW BALLOT
The Battle to Safeguard Democracy in the Age of Electronic Voting

Electronic voting machines, operated with secret software, are unsecure, unreliable and inaccurate. We can no longer trust the results of our elections.

Our democracy is at risk -- citizens must take action and regain control of the electoral process . . .



PROTECT YOUR VOTE

The Help America Vote Act (HAVA) has provided $3.8 billion for voting machine companies whose lobbyists have ensured that no meaningful oversight exists over the privatization of elections.

A massive federal, state and local failure to properly inspect both machines and software has resulted in unsecure, unreliable and inaccurate electronic voting systems being implemented across America.

Only informed citizens, working together, can win back public control of our elections. Here are some of the things you can do:

Get Informed

- Visit election reform websites.
- Search the Web for reports and news articles about electronic voting system problems.
- Ask candidates in public forums where they stand on voter reform efforts. Ask how they will specifically ensure your vote is counted.
- Find out where your federal, state, and local election officials stand on voter reform efforts.

Get Active

- Join a voting reform group, such as the Illinois Ballot Integrity Project.
- Host house parties to share voting reform ideas.
- Become an election judge or pollwatcher.
- Contact legislators and express your concerns about electronic voting systems.

Leave a Paper Trail

- Avoid voting early or by absentee ballot.
- Use a paper ballot instead of a touch-screen.
- If you must use a touch-screen voting machine, be sure to verify your votes on the paper tape.

There are many good online resources to help you become an activist. We suggest you start here:
www.ballot-integrity.org/involved.htm

About the Illinois Ballot Integrity Project

The **Mission** of the **Illinois Ballot Integrity Project** is to inform and educate the public, the media and government officials about important election-integrity issues and to promote the adoption of legislation and policies designed to secure the democratic process.

The **Illinois Ballot Integrity Project** is incorporated as a not-for-profit, non-partisan civic organization dedicated to the correction of election system deficiencies and ensuring fair, accurate, and completely transparent elections.

Join us in the fight for democracy:

IBIP OPEN MEETING - 2ND WEDNESDAY OF THE MONTH from 7- 9 pm
WHOLE FOODS MARKET - 2nd Floor
1000 W. NORTH AVE - CHICAGO

Free, honest, fair and transparent elections are vitally important. And, Americans agree: according to an August 2006 Zogby Poll, 92% of respondents said they want the right to watch votes being counted and to question election officials about how the votes are counted. Whether you oppose the Iraq War, global warming or environmental degradation, or support universal health care, a decent minimum wage or fair immigration policies:

CHANGE ISN'T POSSIBLE UNLESS YOUR VOTE IS COUNTED!

ILLINOIS BALLOT INTEGRITY PROJECT

www.ballot-integrity.org

635 Chicago Ave - Suite 127
Evanston IL 60202
(800) 268-6117
contact@ballot-integrity.org

> **"Vegas slot machines are better monitored and regulated than America's voting machines."**
>
> *- Washington Post*