This is Democracy?:
Problems Voting in America

Ladue Chapel Presbyterian Church

R. Scott Granneman

Denise Lieberman

Denise

Legal Director of ACLU-EM
1997-2005

Washington University in St. Louis

Courts & Civil Liberties

National Security, Civil Liberties & the Law

Gender & Law

Sexuality & Law

Technology & the Law

Senior Attorney

The right to vote freely
for the candidate of one's choice
is of the essence
of a democratic society,
and any restrictions on that right
strike at the heart
of representative government.

Chief Justic Earl Warren
Reynolds v. Sims (1964)


VOTING INSTRUCTIONS
1. START
2. INSTRUCTIONS
3. CHOOSE
4. REVIEW
Please Insert Your Card

Voting

A voting system
has 4 required characteristics

1. Accuracy
2. Anonymity
3. Scalability
4. Speed

Ariel J. Feldman, J. Alex Halderman,
& Edward W. Felten,
Princeton University:

"Simply put,
many computer scientists
doubt that paperless DREs
[Direct Recording Electronic]
can be made reliable and secure,
and they expect
that any failures of such systems
would likely go undetected."

Companies

Company	Localities
ES&S	1,700
Dominion (Diebold/Premier & Sequoia)	600 in 22 states
Hart InterCivic	“Hundreds”

Global Election Systems, Inc. (GES)

↓

Bought by Diebold
(2002 • $24.7 million)

↓

Changes name to Premier Election Solutions
(2007)

↓

Bought by ES&S
(September 2009 • $5 million)

↓

Bought by Dominion Voting Systems
(May 2010 • $?)

ES&S founded
(1979)

↓

Acquires Premier Election Solutions
(September 2009 • $5 million)

↓

Antitrust investigations by DoJ & 14 states

↓

Sells Premier to Dominion Voting Systems
(May 2010 • $?)

Dominion Voting Systems founded
(2002)

↓

Buys Premier Election Solutions from ES&S
(May 2010 • $?)

↓

Buys Sequoia Voting Systems
(June 2010 • $?)

Examples

Diebold, 2003:

“The assertion
that there are any
exploitable attack vectors
is false.
The implication
that malicious code
could be inserted into the system
is baseless.”

Volusia County, FL
2000
Diebold

Voting machine gives Al Gore
–16,022 votes

San Bernardino County, CA
2001

Programming error
causes computers
to look for votes in the wrong place
on a ballot in 33 local elections

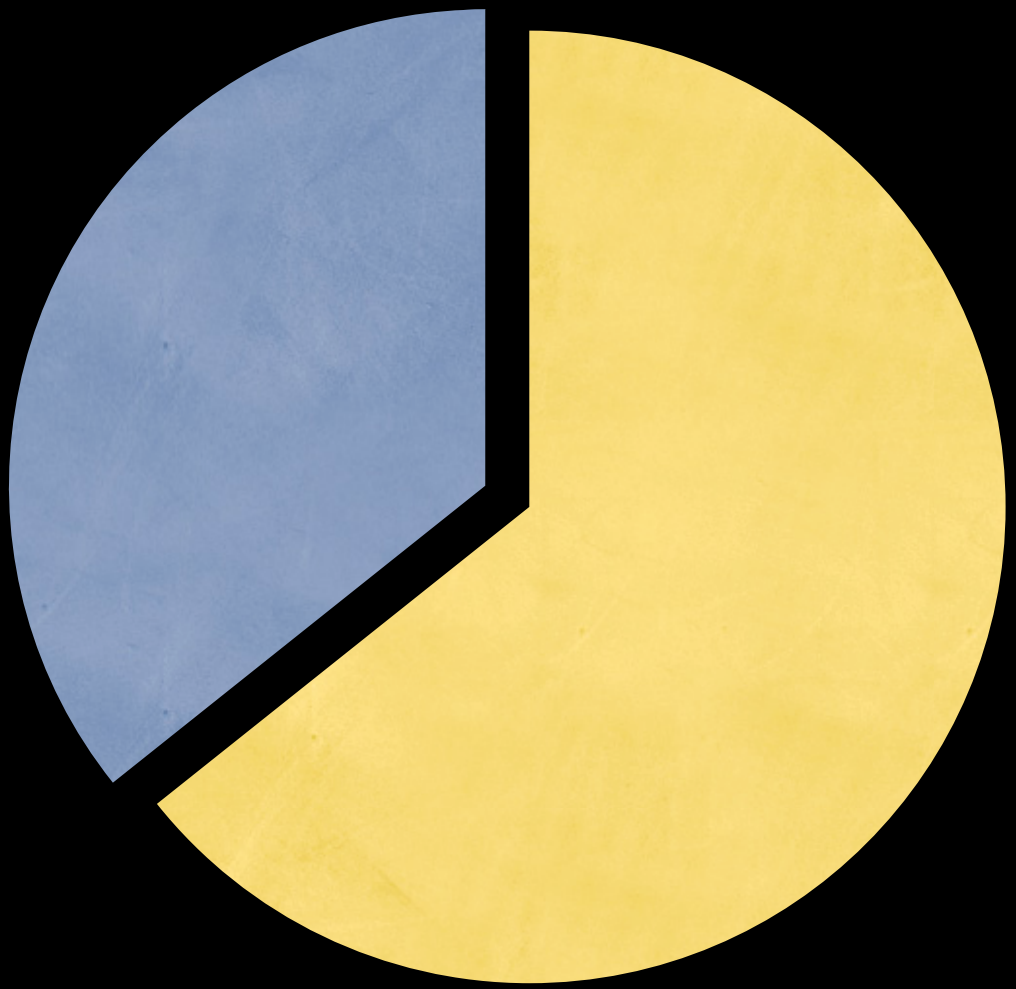
No votes registered for those ballots

Fairfax County, VA
2003

100 votes are subtracted
from one candidate's totals

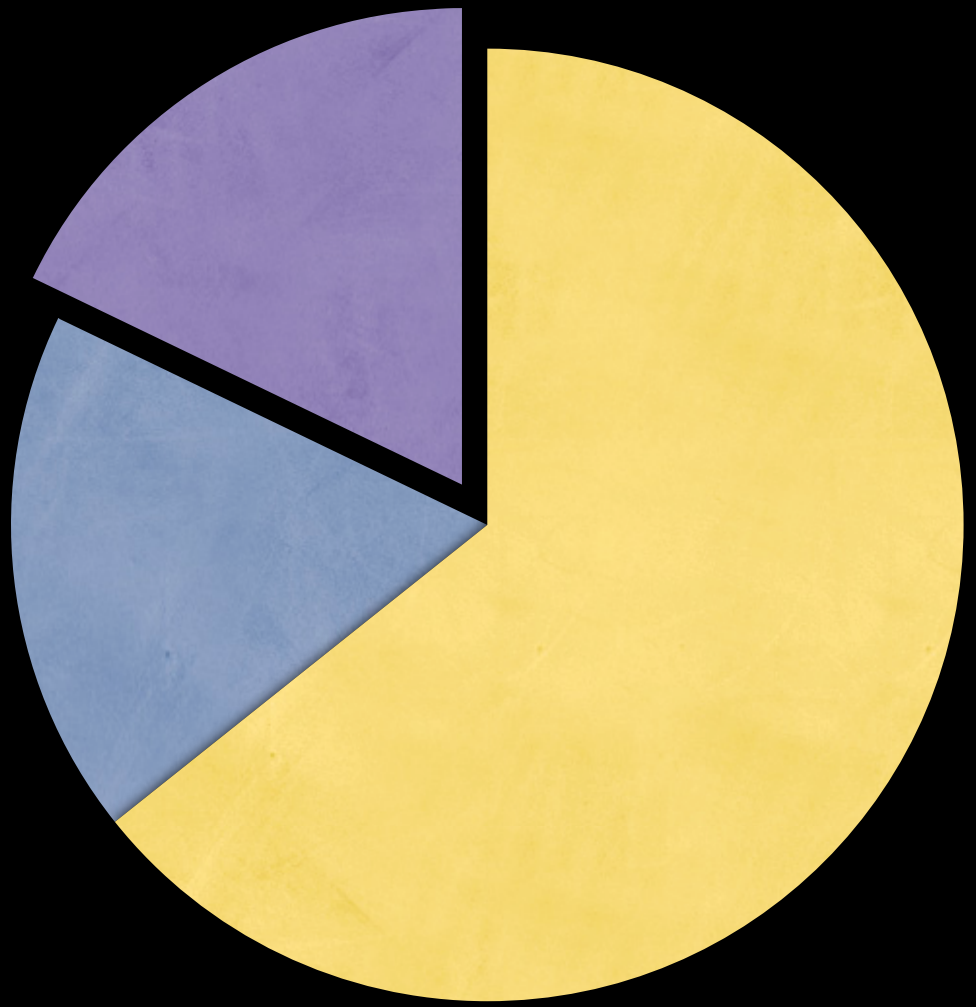
Boone County, IA
2003
140,000 votes counted on machines

Boone County, IA
2003
50,000 people live there



Boone County, IA
2003

25,000 eligible to vote



Palm Beach County, FL
2004

Audits of voting machine logs reveal more than 100,000 errors

✓ Timestamps of 2010
✓ Cards stuck or misread
✓ Powering down (128 times!)
✓ “Unknown event” messages
✓ & many others

Sarasota County, Florida
2006
ES&S

18,000 ballots showed no vote cast in the 13th Congressional District

Undervote rate was 5 times normal

100s of voters complained that day

Race lost by 400 votes

http://blog.wired.com/27bstroke6/2008/10/ess-voting-mach.html

New Jersey
Feb. 2008
Sequoia

5 of New Jersey's 21 counties
report inconsistencies
between numbers of voters reported
& numbers of ballots cast

http://theboard.blogs.nytimes.com/2008/10/24/electronic-voting-the-possibility-of-a-hack/

Jacksonville, FL
2008

“We’re having problems
with the poll machines,”
a voter in Jacksonville, Florida,
told the CNN Voter Hotline.
“They’re not aligned correctly,
so you’re not sure
about which candidate
you’re voting for…”

http://www.cnn.com/2008/POLITICS/10/24/voting.problems/index.html

Jackson County, West Virginia
2008
ES&S

“‘I went in there
and pushed the Democrat ticket,
and it jumped
to the Republican ticket
for president of the United States,’
said Calvin Thomas,
an 81-year-old West Virginian. …”

http://www.cnn.com/2008/POLITICS/10/24/voting.problems/index.html

Jackson County, West Virginia
2008
ES&S

"... The same thing happened to his daughter, Micki Clendenin, when she cast her ballot."

http://www.cnn.com/2008/POLITICS/10/24/voting.problems/index.html

Jackson County, West Virginia
2008
ES&S

Jackson County, West Virginia
2008
ES&S

Decatur County, TN
2008
ES&S

3 voters complain
they voted for McCain
& a vote for Obama was registered

“Voters who are too tall
don’t have a good view of the ballot
and might think
they’re touching the center of the box
when they’re not.”

http://blog.wired.com/27bstroke6/2008/10/ess-voting-mach.html

Mineral Wells, TX
2008
ES&S

Voters report machines switch straight-party vote from Democratic to Republican

http://www.mineralwellsindex.com/local/local_story_298161535.html
http://machinist.salon.com/blog/2008/10/27/early_voting/index.html

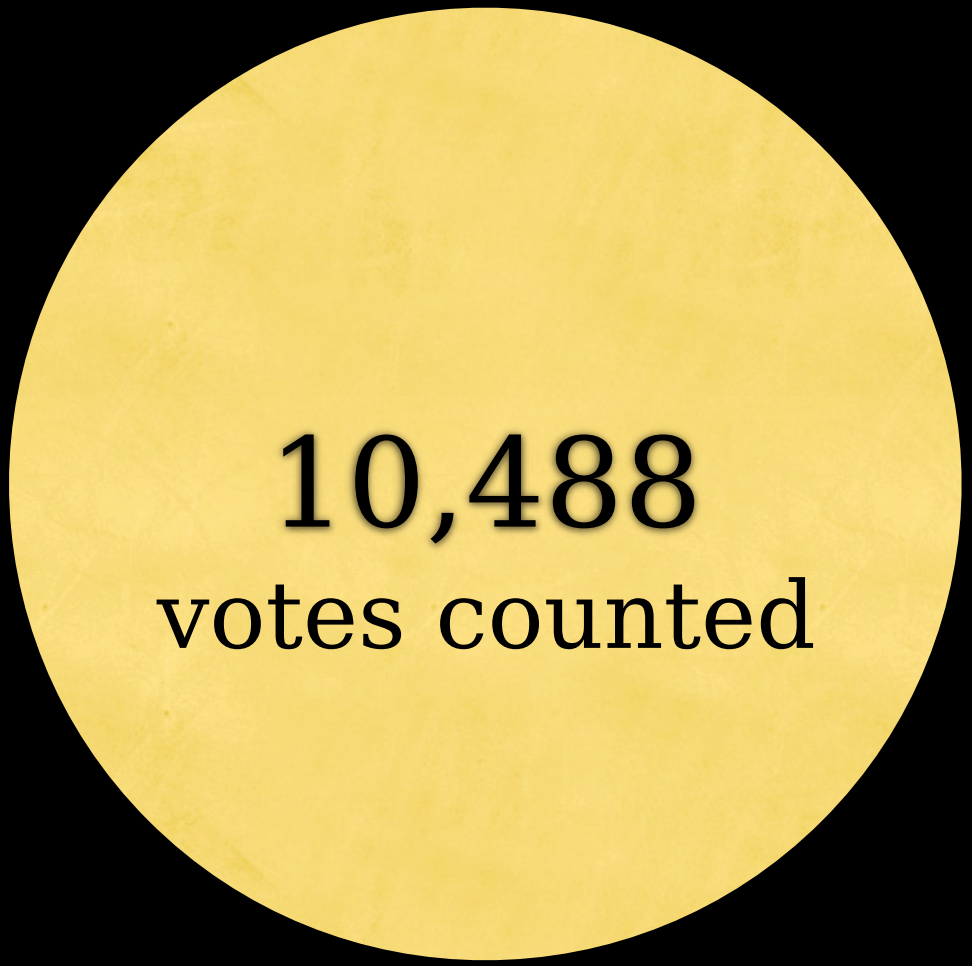
Tennessee
2008
ES&S

Voters have to press
Democrat button
several times

One time it registers vote
for Green Party,
5 rows down

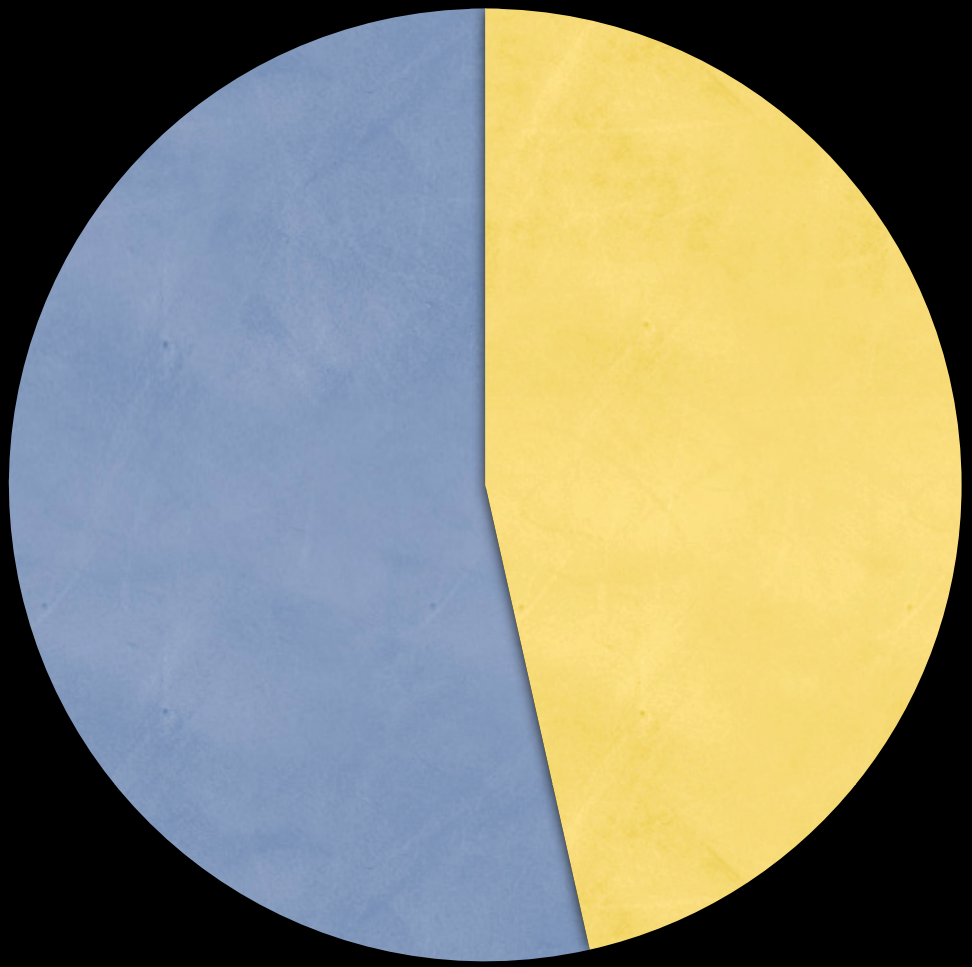
http://machinist.salon.com/blog/2008/10/27/early_voting/index.html
http://www.democracynow.org/2008/10/22/votes

Rapid City, South Dakota
June 2009
ES&S



http://techdirt.com/articles/20090608/2201455173.shtml

Rapid City, South Dakota
June 2009
ES&S



5,613
actual
votes

4,875
phantom
votes

http://techdirt.com/articles/20090608/2201455173.shtml

Diebold

Global Election Systems, Inc. (GES)

↓

Bought by Diebold
(2002 • $24.7 million)

↓

Changes name to Premier Election Solutions
(2007)

↓

Bought by ES&S
(September 2009 • $5 million)

↓

Bought by Dominion Voting Systems
(May 2010 • $?)

The Appearance of Impropriety

2000-2001

Diebold donates more than $195,000 to the Republican party

August 2003

After donating more than $100,000
to the George W. Bush 2004 campaign,
Walden W. O'Dell,
Diebold CEO,
pledges in a fund-raiser invitation:

"I am committed to helping Ohio
deliver its electoral votes
to the president next year."

Alterations Without Notifications

Georgia, 2002

Diebold changes machines' software
8 times
without the state examining it

6 electoral upsets,
including the incumbent senator,
ahead in the polls,
who loses by 11 points

After the election,
Diebold overwrites the flash memory
on all machines' cards

Alameda County, CA
November 2003

Diebold alters software on machines
prior to the elections
without submitting software
for testing
or notifying the state
about the updates

From the Horse's Mouth

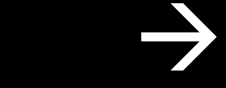
March 2003

Someone breaks into
a Diebold website
& copies 1000s of messages
from an internal discussion board

The messages & source code
are provided to journalists
& posted on college websites

“I need some answers! Our department is being audited by the County. 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.... I would appreciate an explanation on why the memory cards start giving check sum messages. We had this happen in several precincts...”
(18 January 2001)

“Over [the past three years] I have become increasingly concerned about the apparent lack of concern over the practice of writing contracts to provide products and services which do not exist and then attempting to build these items on an unreasonable timetable with no written plan, little to no time for testing, and minimal resources. …



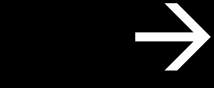
“... It also seems to be an accepted practice to exaggerate our progress and functionality to our customers and ourselves”
(5 October 2001)

“It does not matter whether we get anything certified or not, if we can’t even get the foundation of Global stable. This company is a mess! We should stop development on all new, and old products and concentrate on making them stable instead of showing vaporware. ...

"... You are taxing the development team beyond what they can handle. ... Why is it so hard to get things right! I have never been at any other company that has been so miss managed [sic]."
(20 October 2001)

“For a demonstration [for El Paso County, Colorado] I suggest you fake it. Progam them both so they look the same, and then just do the upload fro [sic] the AV. That is what we did in the last AT/AV [AccuTouch/AccuVote] demo.”
(19 March 1999)

“Right now you can open GEMS’ .mdb file with MS-Access, and alter its contents. That includes the audit log. This isn’t anything new. … Now, where the perception comes in is that its right now very *easy* to change the contents. Double click the .mdb file. …



“... It is possible to put a secret password on the .mdb file to prevent Metamor [a consulting company] from opening it with Access. Being able to end-run the database has admittedly got people out of a bind though. ...

“Jane (I think it was Jane) did some fancy footwork on the .mdb file in Gaston recently. I know our dealers do it. King County is famous for it. That’s why we’ve never put a password on the file before.”
(18 October 2001)

Expert Analysis

Avi Rubin
of Johns Hopkins University
analyzes the Diebold source code

His findings?

It would be easy
for a Diebold insider
to alter the system
to affect votes

Since the code is “closed”,
it could be changed
without detection

All voting machines
use the same hard-coded password

All voting machines
use the same hard-coded password

1111

Without a paper trail,
there is no way to audit the system,
& no way to reconstruct
a disputed election

“Our analysis shows
that this voting system
is far below
even the most
minimal security standards
applicable in other contexts.
We highlight several issues including
unauthorized privilege escalation,
incorrect use of cryptography,
vulnerabilities to network threats, and
poor software development processes.”

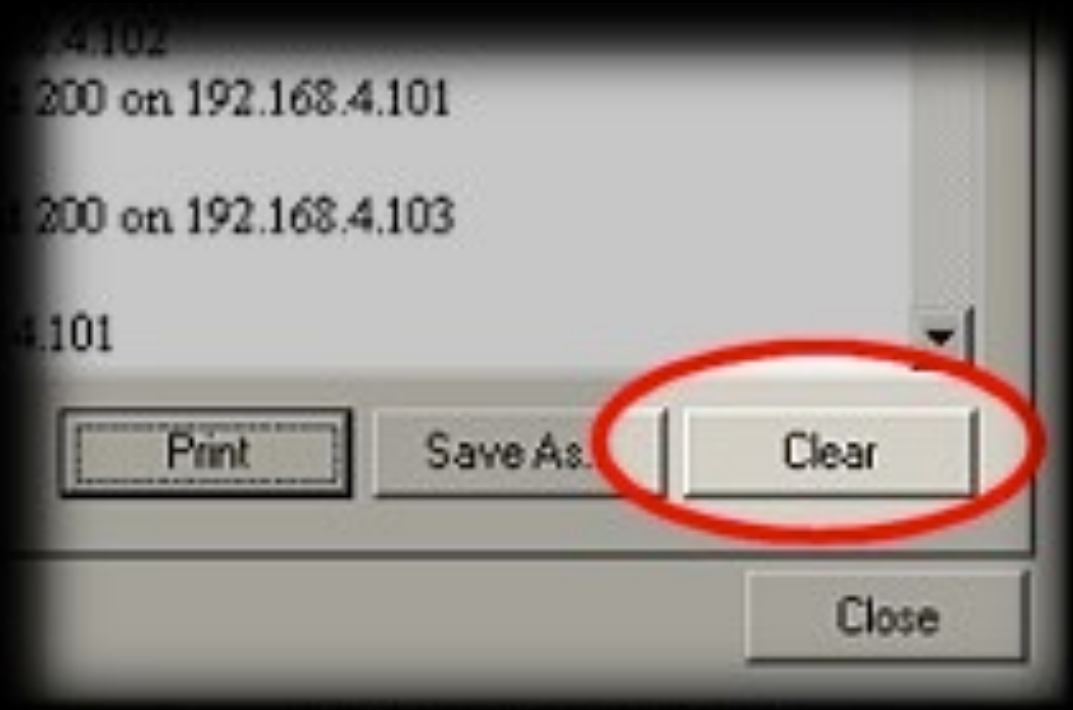
Audit Logs

March 17, 2009

Justin Bales,
Premier's Western Region manager,
at a California state public hearing,
admits the following
about machines used in 34 states:

Audit log system
does not record ballot deletions,
even on election days

Flaws have been present
over a decade



Clear button
deletes the audit log
without asking for confirmation
from the user

Bales of Premier:

"It was just not
in the initial program,
but now
we're taking a serious look at that."

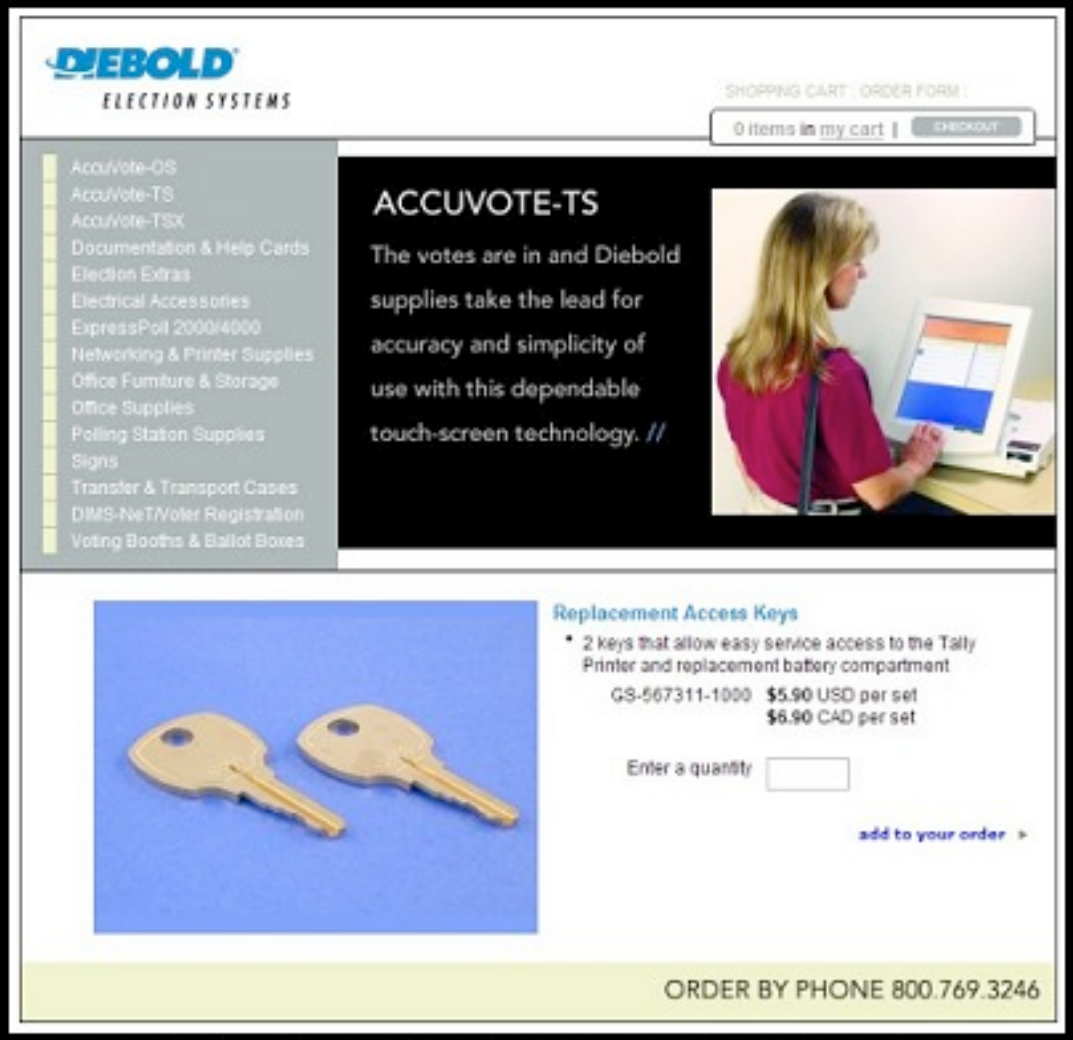
California Secretary of State
on Diebold's audit logs:

"Useless"

Keys

Ed Felten, Princeton:

"The access panel door
on a Diebold
AccuVote-TS voting machine
— the door that protects
the memory card
that stores the votes,
and is the main barrier
to the injection of a virus —
can be opened with a standard key
that is widely available on the Internet."



IS DIEBOLD THE DUMBEST COMPANY IN THE HISTORY OF AMERICA?

Screenshot from Diebold's online web store featuring a photo of the key used to open every one of their "secure", yet incredible hackable, electronic voting machines. Working copies were made from only the photo above and used to open a Diebold AccuVote TS system.

The BRAD BLOG | BradBlog.com

Problems

Expensive

April 2009

Ireland announces
it’s abandoning electronic voting
& going back to paper

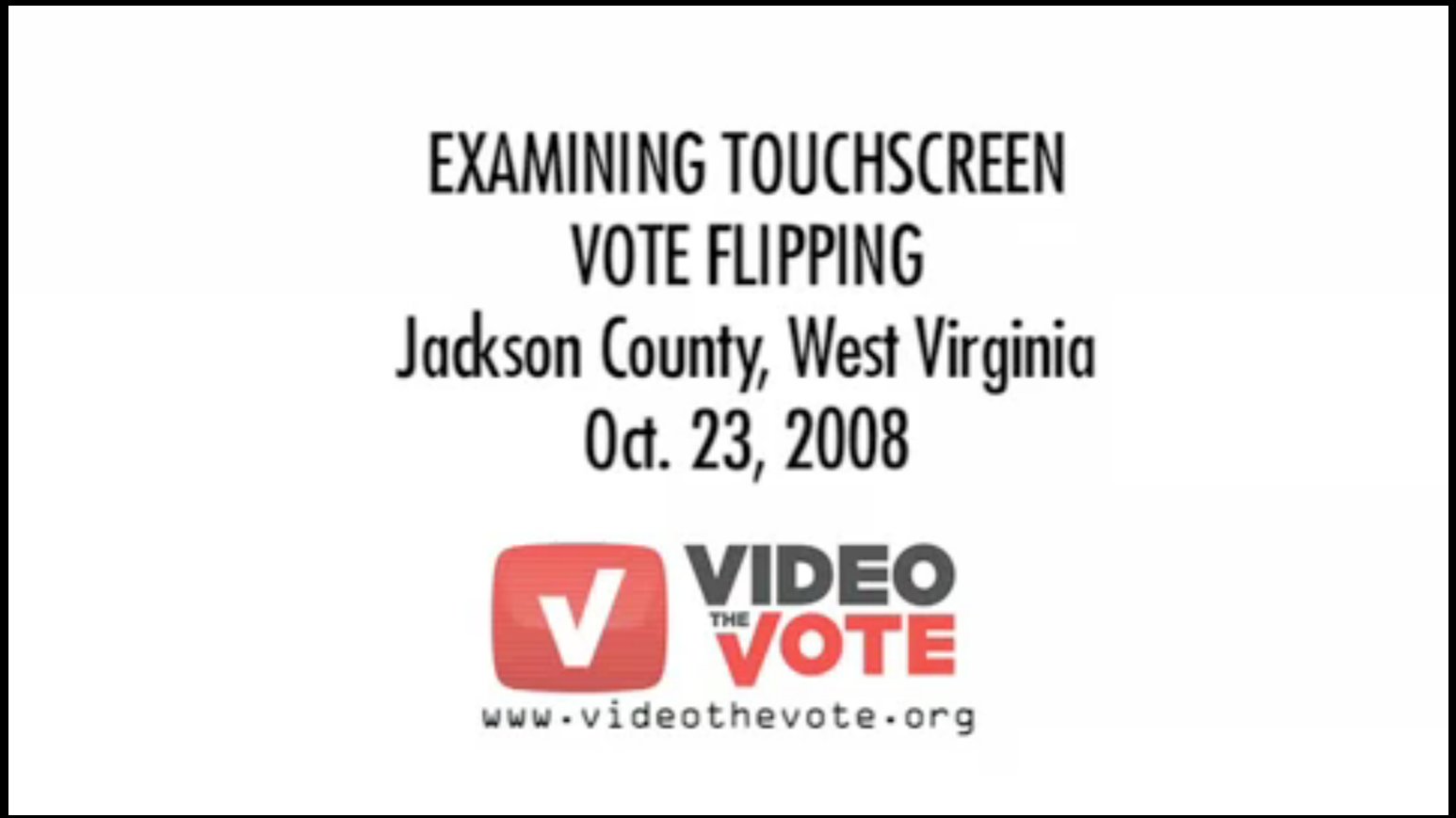
$67,000,000 loss

http://arstechnica.com/tech-policy/news/2009/04/irish-reject-e-voting-go-back-to-paper.ars

Calibration

Jackson County, WV
Clerk Jeff Waybright
2008
ES&S

Jackson County, WV
Clerk Jeff Waybright
2008
ES&S



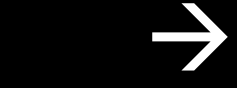
Hackability

From *Security Analysis of the Diebold AccuVote-TS Voting Machine*:

"1. Malicious software running on a single voting machine can steal votes with little if any risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss.

“We have constructed demonstration software that carries out this vote-stealing attack.

“2. Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute. In practice, poll workers and others often have unsupervised access to the machines.



“3. AccuVote-TS machines are susceptible to voting-machine viruses—computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre- and post-election activity. We have constructed a demonstration virus that spreads in this way, installing our demonstration vote-stealing program on every machine it infects.”

Dan S. Wallach,
Associate Prof. of Computer Science,
Rice University

"What we learned from
the California Top-to-Bottom Review
and the Ohio EVEREST study
was that, indeed, these systems are
unquestionably and unconscionably
insecure."

http://techdirt.com/articles/20090417/0214474537.shtml

When machine boots,
it checks to see if `fboot.nb0`
is on removable memory card

If it is, the machine
replaces bootloader code
on its on-board flash memory
with new `fboot.nb0`

When machine boots,
it checks to see if `explorer.glb`
is on removable memory card

If it is,
the machine runs `explorer.glb`
without any authentication

Operating system
used by Diebold voting machines:

Operating system
used by Diebold voting machines:

Windows CE 3.0

Uniformity

Millions of copies
of the same machines
are in use across the USA

One problems means that
elections across the country
would be affected

Infrastructure

What if the electricity fails?

The Biggest Problem


'02 8

Solutions

Better Security Procedures

In the Netherlands,
after a voting foundation
demonstrated security holes,
the Dutch government
ordered all software to be replaced,
all hardware to be checked,
unflashable firmware to be installed,
& iron seal to be placed on machines

Machines were checked randomly
on election day

Paper ballots must always
be available,
enough for everyone to use
if necessary

Open Source

What's *open source*?

Secrecy does not mean security

Brazil, 2008

128 million people
used locally-developed,
Linux-based voting machines
to vote for 5000 city mayors

Australia

eVACS
Electronic Voting and Counting System

Open source code
that runs on Linux

Phillip Green, electoral commissioner for Australian Capital Territory:

“We’d been watching what had happened in America, and we were wary of using proprietary software that no one was allowed to see.

“We were very keen for the whole process to be transparent so that everyone—particularly the political parties and the candidates, but also the world at large—could be satisfied that the software was actually doing what it was meant to be doing.”

Los Angeles election official:

“The software developed for InkaVote is proprietary software. All the software developed by vendors is proprietary. I think it’s odd that some people don’t want it to be proprietary. If you give people the open source code, they would have the directions on how to hack into it. We think the proprietary nature of the software is good for security.”

Bruce Schneier:

“What she should be saying is something like: ‘I think it’s odd that everyone who has any expertise in computer security doesn’t want the software to be proprietary. Speaking as someone who knows nothing about computer security, I think that secrecy is an asset.’”

Dan S. Wallach,
Associate Prof. of Computer Science,
Rice University

“Disclosing the source code only results in a complete forfeiture of the software’s security if there was never any security there in the first place. …

“If the product is well-engineered, then disclosing the software will cause no additional security problems. If the product is poorly-engineered, then the lack of disclosure only serves the purpose of delaying the inevitable.”

Voter-verified paper trails

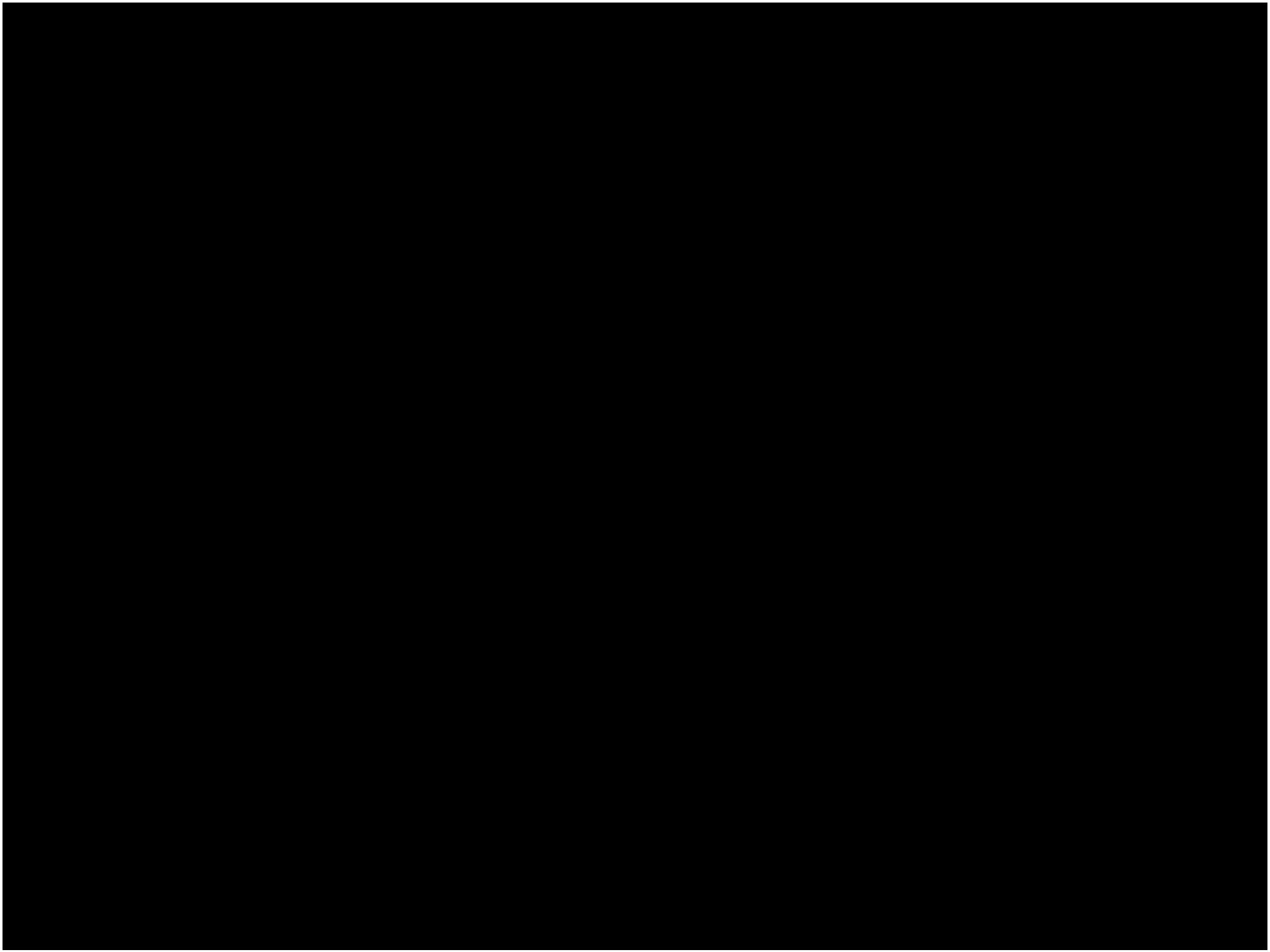
Independent security reviews
of hardware & software

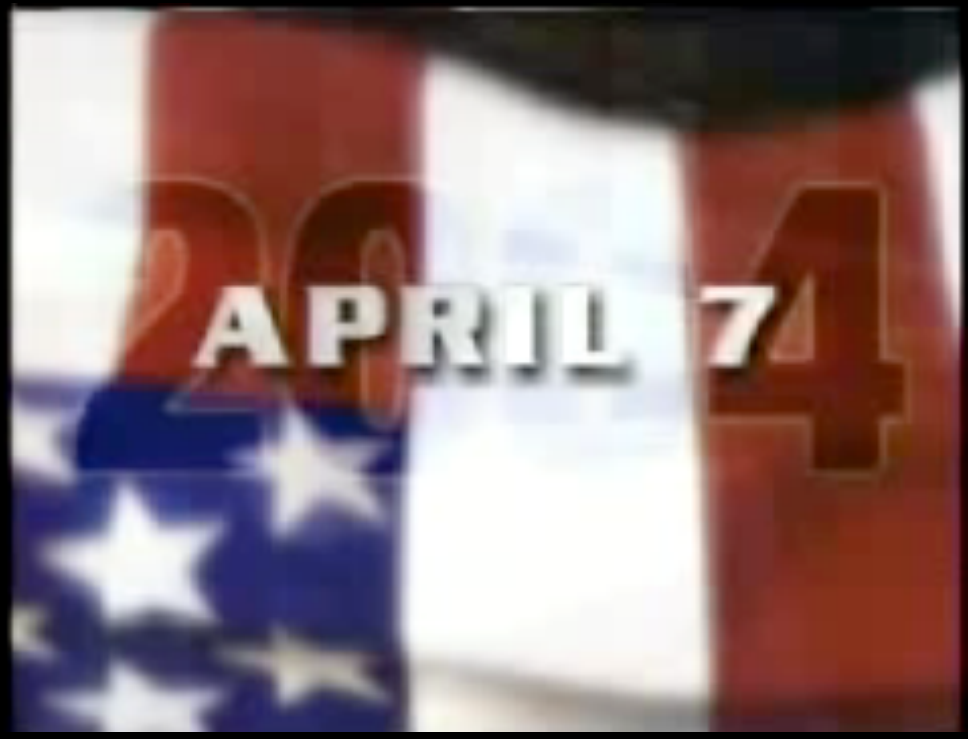
Learn

Bruce Schneier

Edward Felten

Avi Rubin




APRIL 7

Thank you!

Email: scott@granneman.com

Web: www.granneman.com

Publications: www.granneman.com/pubs

Blog: blog.granneman.com

Twitter: scottgranneman

Email: denise@deniselieberman.com

This is Democracy?:
Problems Voting in America

Ladue Chapel Presbyterian Church

R. Scott Granneman

Denise Lieberman

Licensing of this work

Questions? Email scott@granneman.com