

1 Cindy A. Cohn, Esq. (SBN 145997)
Wendy Seltzer, Esq.
2 ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
3 San Francisco, CA 94110
Telephone: (415) 436-9333 x108
4 Facsimile: (415) 436-9993
5 Attorneys for Plaintiff
ONLINE POLICY GROUP

6 Jennifer Stisa Granick, Esq. (SBN 168423)
7 STANFORD LAW SCHOOL
CENTER FOR INTERNET & SOCIETY
8 559 Nathan Abbott Way
Stanford, CA 94305-8610
9 Telephone: (650) 724-0014
Facsimile: (650) 723-4426

10 Attorneys for Plaintiffs
NELSON CHU PAVLOSKY and LUKE
THOMAS SMITH

12 UNITED STATES DISTRICT COURT

13 FOR THE NORTHERN DISTRICT OF CALIFORNIA

14 ONLINE POLICY GROUP, NELSON CHU)
15 PAVLOSKY, and LUKE THOMAS SMITH,)

16 Plaintiffs,)

17 v.)

18 DIEBOLD, INCORPORATED, and DIEBOLD)
19 ELECTION SYSTEMS, INCORPORATED,)

20 Defendants.)

No.

**DECLARATION OF WENDY SELTZER
IN SUPPORT OF PLAINTIFFS'
APPLICATION FOR TEMPORARY
RESTRAINING ORDER AND FOR
PRELIMINARY INJUNCTION**

21 I, Wendy Seltzer, hereby declare as follows.

22 I am an attorney with the Electronic Frontier Foundation, counsel to Plaintiff Online
23 Policy Group. I make this Declaration in support of plaintiff's application for a temporary
24 restraining order and for a preliminary injunction.

25 2. On the morning of Monday, November 3, 2003, at 9:00 a.m., called Diebold
26 attorney Ralph E. Jocke to give notice of Plaintiffs' application for temporary restraining order and
27 for preliminary injunction. I left a message to that effect with the receptionist. I sent facsimile
28 copies of our papers to Mr Jocke at 330-723-6446 and emailed copies to

1 rej@walkerandjocke.com. I further caused the papers to be served on Diebold, Inc. and Diebold
2 Election Systems, Inc. through their registered agent: CT Corp. Systems, 818 West Seventh Street,
3 Los Angeles, CA 90017.

4 3. Attached hereto as Exhibit A is a true and correct copy of the letter I wrote on
5 behalf of Online Policy Group to Diebold attorney Ralph E. Jocke, which sent to him by e-mail
6 and U.S. mail on October 22, 2003.

7 4. Attached hereto as Exhibit B is a printout of what am informed and believe to be
8 the Diebold e-mail archive that was posted on the Swarthmore Coalition for the Digital Commons
9 website and that was linked to from the San Francisco IndyMedia website.

10 5. Attached hereto as Exhibit C is a true and correct copy of a newspaper article: John
11 Schwartz, *Computer Voting Is Open to Easy Fraud, Experts Say*, N.Y. TIMES, July 24, 2003 at
12 A16.

13 6. Attached hereto as Exhibit D is a true and correct copy of a newspaper article:
14 Nelson Hernandez & Lori Montgomery, *Md. Democrats Want Outside Voting Machine Audit*,
15 WASH. POST, October 21, 2003 at B01

16 7. Attached hereto as Exhibit E is a true and correct copy of a newspaper article:
17 Rachel Konrad (Associated Press), *Diebold issues threats to publishers of leaked documents*, SAN
18 JOSE MERCURY NEWS, October 28, 2003

19 8. Attached hereto as Exhibit F is a true and correct copy of a magazine article: Steven
20 Levy, *Black Box Voting Blues*, NEWSWEEK, October 2003, at
21 <<http://www.msnbc.com/news/985033.asp>>

22 9. Attached hereto as Exhibit G is a true and correct copy of a newspaper article:
23 Kristin Smith, *Swarthmore students refuse to comply with Diebold Co.*, DELAWARE COUNTY DAILY
24 TIMES, October 24, 2003 at 7.

25 10. Attached hereto as Exhibit H is a true and correct copy of a printout from Ed
26 Foster's GripeLog, "Latest DMCA Takedown Victim: The Election Process," October 30, 2003

27 11. Attached hereto as Exhibit I is a true and correct copy of a news article: Associated
28 Press, *Worries grow over new voting machines' reliability, security*, CNN.COM, October 30, 2003,

1 at <<http://www.cnn.com/2003/ALLPOLITICS/10/30/elec04.election.worries/>>.

2 12. Attached hereto as Exhibit J is a true and correct copy of a printout from the Why-
3 War? website, as of November 2, 2003, listing mirrors of the e-mail archive and indicating those
4 for which takedown requests have been received:

5 <<http://www.why-war.com/features/2003/10/diebold.html>>

6 I declare under penalty of perjury under the laws of the State of California that the
7 foregoing is true and correct and that this declaration was executed in San Francisco, California.

8
9 Date: Nov. 3, 2003


WENDY SELTZER



Electronic Frontier Foundation
Protecting Rights and Promoting Freedom on the Electronic Frontier

October 22, 2003

Ralph E. Jocke, Esq.
Walker & Jocke
231 South Broadway
Medina, Ohio 44256

VIA EMAIL (rej@walkerandjocke.com) AND U.S. MAIL

RE: Diebold's Copyright Infringement Claim

Dear Mr. Jocke

The Electronic Frontier Foundation represents the Online Policy Group (OPG), a non-profit Internet service provider. Please provide all future correspondence on this issue to us. After review of your letter of October 10, 2003, to William Doherty, OPG respectfully declines to remove the IndyMedia pages you reference therein.

First, OPG is merely providing co-location to IndyMedia, which in turn is only providing hyperlinks to materials you claim infringe Diebold copyrights. In other words, OPG does not host the Diebold materials and neither does IndyMedia. There is merely an address for the information on the IndyMedia website as source material for a news story. Linking is not among the exclusive rights granted by the Copyright Act, 17 U.S.C. §106, and so cannot infringe any copyright Diebold might hold. Your allegations amount to a claim of tertiary liability; copyright law does not reach parties so far removed from a claimed infringement.

Second, the postings themselves are plainly fair use, not infringement. As the Copyright Act provides, "the fair use of a copyrighted work ... for purposes such as criticism, comment, news reporting, ... or research, is not an infringement of copyright." 17 U.S.C. § 107. IndyMedia is a news organization whose use of these links gives background to its discussion of the controversy surrounding e-voting. We understand that the linked-to material contains internal memoranda concerning Diebold's electronic voting machines, including admissions by Diebold staff of errors, difficulties, bugs and other problems with the machines and software. We further understand that IndyMedia linked to these memoranda as part of news reportage about the risks of election fraud or erroneous election results that might arise from use of Diebold's voting machines.

The First Amendment plainly protects speech about this very essence of our democracy -- the right to a free and fair election. Thus, even if Diebold has an enforceable copyright in the documents, their reposting by others serves the public interest and would be deemed fair and non-infringing on all four factors of the fair use analysis: 1) The purpose and character of the use is to inform public discussion and political debate on a matter core to American democracy, the functioning of our electoral system. As a news agency, IndyMedia should be able to link to its primary sources. 2) The nature of the work is (presumably) factual and thus less protected. 3) The documents do not appear to embody any substantial expressive work. 4) Most importantly, the posting does not compete with Diebold in any current or potential market -- if it

October 22, 2003

Page 2

cuts into sales of e-voting equipment, it does so only because Diebold's own statements have raised concerns about the machines' security.

Finally, it appears you are harassing numerous ISPs with these frivolous demand letters, misusing claimed copyright to interfere with numerous subscribers' contracts for Internet service. You may wish to consider the risk of countersuit at which this puts you and your client.

Please contact me directly if you wish to discuss the matter further.

Sincerely,

A handwritten signature in black ink, appearing to read "Wendy Seltzer", with a long horizontal line extending to the right.

Wendy Seltzer



July 24, 2003

Computer Voting Is Open to Easy Fraud, Experts Say

By JOHN SCHWARTZ

The software that runs many high-tech voting machines contains serious flaws that would allow voters to cast extra votes and permit poll workers to alter ballots without being detected, computer security researchers said yesterday.

"We found some stunning, stunning flaws," said Aviel D. Rubin, technical director of the Information Security Institute at Johns Hopkins University, who led a team that examined the software from Diebold Election Systems, which has about 33,000 voting machines operating in the United States.

The systems, in which voters are given computer-chip-bearing smart cards to operate the machines, could be tricked by anyone with \$100 worth of computer equipment, said Adam Stubblefield, a co-author of the paper.

"With what we found, practically anyone in the country — from a teenager on up — could produce these smart cards that could allow someone to vote as many times as they like," Mr. Stubblefield said.

The software was initially obtained by critics of electronic voting, who discovered it on a Diebold Internet site in January. This is the first review of the software by recognized computer security experts.

A spokesman for Diebold, Joe Richardson, said the company could not comment in detail until it had seen the full report. He said that the software on the site was "about a year old" and that "if there were problems with it, the code could have been rectified or changed" since then. The company, he said, puts its software through rigorous testing.

"We're constantly improving it so the technology we have 10 years from now will be better than what we have today," Mr. Richardson said. "We're always open to anything that can improve our systems."

Another co-author of the paper, Tadayoshi Kohno, said it was unlikely that the company had plugged all of the holes they discovered.

There is no easy fix Mr. Kohno said

The move to electronic voting — which intensified after the troubled Florida presidential balloting in 2000 — has been a source of controversy among security researchers. They argue that the companies should open their software to public review to be sure it operates properly.

Mr. Richardson of Diebold said the company's voting-machine source code, the basis of its computer program, had been certified by an independent testing group. Outsiders might want more access, he said, but "we don't feel it's necessary to turn it over to everyone who asks to see it, because it is proprietary."

Diebold is one of the most successful companies in this field. Georgia and Maryland are among its clients, as are many counties around the country. The Maryland contract, announced this month, is worth

\$56 million

Diebold, based in North Canton, Ohio, is best known as a maker of automated teller machines. The company acquired Global Election Systems last year and renamed it Diebold Election Systems. Last year the election unit contributed more than \$110 million in sales to the company's \$2 billion in revenue.

As an industry leader, Diebold has been the focus of much of the controversy over high-tech voting. Some people, in comments widely circulated on the Internet, contend that the company's software has been designed to allow voter fraud. Mr. Rubin called such assertions "ludicrous" and said the software's flaws showed the hallmarks of poor design, not subterfuge.

The list of flaws in the Diebold software is long, according to the paper, which is online at avirubin.com/vote.pdf. Among other things, the researchers said, ballots could be altered by anyone with access to a machine, so that a voter might think he is casting a ballot for one candidate while the vote is recorded for an opponent.

The kind of scrutiny that the researchers applied to the Diebold software would turn up flaws in all but the most rigorously produced software, Mr. Stubblefield said. But the standards must be as high as the stakes, he said.

"This isn't the code for a vending machine," he said. "This is the code that protects our democracy

Still, things that seem troubling in coding may not be as big a problem in the real world, Mr. Richardson said. For example, counties restrict access to the voting machines before and after elections, he said. While the researchers "are all experts at writing code, they may not have a full understanding of how elections are run," he said.

But Douglas W. Jones, an associate professor of computer science at the University of Iowa, said he was shocked to discover flaws cited in Mr. Rubin's paper that he had mentioned to the system's developers about five years ago as a state elections official.

find that such flaws have not been corrected in half a decade is awful," Professor Jones said

Peter G. Neumann, an expert in computer security at SRI International, said the Diebold code was "just the tip of the iceberg" of problems with electronic voting systems.

This is an iceberg that needs to be hacked at a good bit Mr. Neumann said so this is a step forward

washingtonpost.com go to mywashingtonpost

Home News Politics Entertainment Live Discussions Photos Marketplace Jobs

▼ ADVERTISING

Navigate to Sections **SEARCH: News** Search Options

GO GO

[News](#) > [Metro](#) > [Maryland](#) > [Government](#)

Md. Democrats Want Outside Voting Machine Audit

By *Nelson Hernandez and Lori Montgomer*
Washington Post Staff Writers
Tuesday, October 21, 2003; Page B01

Democratic legislative leaders called yesterday for independent auditors to study problems with Maryland's voting machines, saying they do not trust Republican Gov. Robert L. Ehrlich Jr. to resolve the matter on his own.

▼ ADVERTISING In a letter to the director of the Maryland Department of Legislative Services, Sen. Paula C. Hollinger (D-Baltimore County) and Del. Sheila Ellis Hixson (D-Montgomery) asked that the agency examine a report issued in September by Science Application International Corp. on security weaknesses in a new computerized voting system the state is prepared to purchase for \$55.6 million.

The SAIC report on the system, developed by Diebold Elections Systems Inc., found serious flaws that could allow tampering with election results. The study was a response to a July report by Johns Hopkins University computer scientist Aviel Rubin and colleagues who said the voting system was vulnerable to manipulation.

The report led Diebold to tighten the security of its software, but Democrats questioned the impartiality of SAIC, the research company chosen by the Ehrlich administration. The San Diego-based firm has had a standing contract with the state government since 2002 for information technology consulting.

"We first want to know what's going on," said Hollinger, who chairs the Senate committee that oversees electoral issues. "The legislature has not been involved at all. Whether there's a problem or not, the only way to determine it is we do it independently.

"Elections are for everybody, 'D's and 'R's and 'I's and everybody else on the ballot. In the next election, everybody ought to feel it's not influenced by partisanship."

To that end, Hollinger and Hixson asked the legislative agency to examine the process used to select the firm to conduct the review of the Diebold system and the Johns Hopkins report and to report on "the professional credentials and organizational composition of SAIC to ensure that the SAIC analysis was objective, balanced, impartial, and free of outside influence or other conflicts."

Company officials referred all questions to Ehrlich's office, where a spokesman said the governor welcomes the new report.

"We're confident in the SAIC review," said Henry Howell.

[Free E-mail Newsletters](#)
[News Headlines News Alert](#)

[E-Mail This Article](#)
[Printer-Friendly Version](#)
[Permission to Republish](#)
[Subscribe to The Post](#)

In recent weeks, some Democrats have expressed concerns that the problems with the voting machines would be used to drive out State Board of Elections Administrator Linda H. Lamone, a Democrat appointed by Ehrlich's predecessor, Parris N. Glendening (D), and replace her with a Republican. Lamone was at a conference yesterday and could not be reached.

Karl S. Aro, executive director of the Department of Legislative Services, said that his agency would respond to the request, but he noted that the deadline set for his report -- Jan. 12, near the start of the legislative session -- might be too close.

"We will look at it," Aro said. "We'll see exactly what they're asking us to do."

© 2003 The Washington Post Company

Privacy blocked
http://pagead2.googlesyndication.com/pagead/ads?client=ca-washingtonpost_416x144&randor
See why or go there anyway.

[News](#) > [Metro](#) > [Maryland](#) > [Government](#)

Navigate the Metro Section ▾

GO

Navigate to Sections ▾

GO

SEARCH:

News ▾

Search
Options

GO

ADVERTISING

washingtonpost

my.washingtonpost

Home

News

Politics

Entertainment

Live Discussions

Photos

Marketplace

Jobs



Silicon Valley.com

El Nuevo Mundo

[Contact Us](#) | [Site Index](#) | [Archives](#) | [Place an Ad](#) | [Newspaper Subscriptions](#) | [News by Email](#)

 Search Articles-last 7 days for
[Shopping & Services](#)

 Find a [Job](#), a [Car](#),
an [Apartment](#),
a [Home](#), and more...

Find It Fast

- [Traffic Reports](#)
- [Weather](#)
- [News](#)
- [Obituaries](#)
- [Editorials](#)
- [Classifieds](#)
- [Sports](#)
- [Business](#)
- [Entertainment](#)
- [Lifestyles](#)
- [Newspaper Ads Online](#)

[Back to Home](#) > [News](#) >

Sunday, Nov 02, 2003

Local News

Posted on Tue, Oct. 28, 2003

Diebold issues threats to publishers of leaked documents

 RACHEL KONRAD
Associated Press

SAN JOSE, Calif. - One of the nation's largest electronic voting machine suppliers is threatening to sue activists for publishing leaked company documents that they claim raise serious security questions.

But despite legal threats from Diebold Inc., some activists are refusing to remove the documents from Web sites.

Diebold sent "cease and desist" letters after the documents and internal e-mails, allegedly stolen by a hacker, were distributed on the Internet. Recipients of the letters included computer programmers, students at Swarthmore College and at least one Internet provider.

Most of the 13,000 pages of documents are little more than banal employee e-mails, routine software manuals and old voter record files. But several items appear to raise security concerns.

Diebold refused to discuss the documents' contents. Company spokesman Mike Jacobsen said the fact that the company sent the cease-and-desist letters does not mean the documents are authentic - or give credence to advocates who claim lax Diebold security could allow hackers to rig machines.

"We're cautioning anyone from drawing wrong or incomplete conclusions about any of those documents or files purporting to be authentic," Jacobsen said.

CONTACT US

The news desk
Complete staff list

TOOLS

- » [Yellow Pages](#)
- » [Discussion Boards](#)
- » [Map and Directions](#)
- » [Mercury News Mortgage Watch](#)

SPECIAL PACKAGES

- » [Governor recall](#)
- » [Budget Crisis](#)
- » [Laci Peterson murder trial](#)
- » [Iraq: The Aftermath](#)
- » [Juvenile Hall abuse allegations](#)
- » [Silicon Valley's top 150 companies](#)
- » [Irvine Foundation investigation](#)
- » [Inside Google: A new dot-com generation](#)

SOMETHING TO SAY?

- » [Talk about it in our news forums](#)

News

- [Local News](#)
- [San Jose/Valley](#)
- [Central Coast](#)
- [Peninsula](#)
- [Alameda County](#)
- [California & the West](#)
- [Nation/World](#)
- [Obituaries](#)
- [Education](#)
- [Science & Health](#)
- [Weird News](#)
- [Special Reports](#)
- [Iraq: The Aftermath](#)

Classifieds

- [Automotive](#)
- [Real Estate](#)
- [Employment](#)
- [Personals](#)

Opinion

- [Perspective](#)
- [Columnists](#)

Business

- [Financial Markets](#)
- [Technology](#)
- [Personal Technology](#)
- [Personal Finance](#)
- [People and Events](#)
- [Drive](#)
- [Sports](#)
- [San Francisco 49ers](#)
- [Oakland Raiders](#)

- **San Francisco Giants**
- **Oakland Athletics**
- **Golden State Warriors**
- **San Jose Sharks**
- **High school sports**
- **College sports**
- **Soccer**
- **Golf**
- **Motorsports**
- **Other sports**
- **Outdoors**
- **Entertainment**
- **Books**
- **Celebrities**
- **Comics and Games**
- **Dining**
- **Events**
- **Eye**
- **Horoscopes**
- **Movies**
- **Music**
- **Nightlife**
- **Performing Arts**
- **TV**
- **Visitors Guide**
- **Visual Arts**
- **Lifestyles**
- **Family & Religion**
- **Food & Wine**
- **Home & Garden**
- **Style**
- **Travel**

But the activists say the mere fact that Diebold was hacked shows that the company's technology cannot be trusted.

"These legal threats are an acknowledgment of the horrific security risks of electronic voting," said Sacramento-based programmer Jim March, who received a cease and desist order last month but continues to publish the documents on his personal Web site.

In one series of e-mails, a senior engineer dismisses concern from a lower-level programmer who questions why the company lacked certification for a customized operating system used in touch-screen voting machines.

The Federal Election Commission requires voting software to be certified by an independent research lab.

In another e-mail, a Diebold executive scolded programmers for leaving software files on an Internet site without password protection.

"This potentially gives the software away to whomever wants it," the manager wrote in the e-mail.

March contends the public has a right to know about Diebold security problems.

"The cease-and-desist orders are like a drug dealer saying, 'Hey, cop, give me back my crack.' It's an incredible tactical blunder," he said.

The documents began appearing online in August, six months after a hacker broke into the North Canton, Ohio-based company's servers using an employee's ID number, Jacobsen said. The hacker copied company announcements, software bulletins and internal e-mails dating back to January 1999, Jacobsen said.

In August, someone e-mailed the data to electronic-voting activists, many of whom published stories on their Web logs and personal sites. A freelance journalist at Wired News, Brian McWilliams, also received data and wrote about it in an online story.

The data was further distributed in digital form around the Internet and it is not known how many copies exist.

Wendy Seltzer, an attorney for the Electronic Frontier Foundation, said she has been contacted by about a dozen groups that received cease-and-desist letters. Among them is Online Policy Group, a nonprofit ISP that hosts the San Francisco Bay Area Independent Media Center, which published links to the data.



WAR PHOTOS

Check out amazing Iraq war photos from staff photographer Pauline Lubens.

LOOKING FOR .

- » **Special reports**
- » **Local news**
- » **California news**
- » **Politics**

Seltzer encouraged them to defy the Diebold
cease-and-desist letters.

"There is a strong fair-use defense," Seltzer said. "People are
using these documents to talk about the very mechanism of
democracy - how the votes are counted. It's at the heart of
what the First Amendment protects."



[email this](#)



[print this](#)



© 2003 Knight Ridder
Mercury News
All rights reserved.

[Contact Us](#) | [Site Index](#) | [Archives](#) | [Place an Ad](#) | [Newspaper Subscriptions](#) | [News by Email](#)
[About The Mercury News](#) | [About the Real Cities Network](#) | [Terms of Use & Privacy Statement](#)
[About Knight Ridder](#) | [Copyright](#)

The screenshot shows the MSNBC News website interface. At the top, there are navigation links: MSN Home, My MSN, Hotmail, Search, Shopping, Money, and People & Chat. Below these is the MSNBC News logo. A sidebar on the left lists categories under 'INSIDE NEWSWEEK': Periscope, National, World, Business, Tech • Science, Health • Life, Entertainment, Columnists, Tip Sheet, Arts & Opinions, and Intl. Editions. The main content area features the Newsweek logo and a navigation bar with links to Home Page, Cover Story, Archives, Feedback, and Index. Below this is a section titled 'Technology & Science' with a sub-section 'RANDOM ACCESS' featuring a portrait of Steven Levy. A small credit 'Sigrd Estrada' is visible at the bottom right of the image.

Advertisement

QwestDex
online yellow pages
Find a Local Business

Black Box Voting Blues

Electronic ballot technology makes things easy. But some computer-security experts warn of the possibility of stolen elections

By Steven Levy
NEWSWEEK

Nov. 3 issue — After the traumas of butterfly ballots and hanging chad, election officials are embracing a brave new ballot: sleek, touch-screen terminals known as direct recording electronic voting systems (DRE). States are starting to replace their Rube Goldbergesque technology with digital devices like the Diebold Accu-Vote voting terminal. Georgia uses Diebolds exclusively, and other states have spent millions on such machines, funded in part by the 2002 federal Help America Vote Act. Many more terminals are on the way.

Newsweek Technology and Science

- Welcome to History 2.0
- Black Box Voting Blues
- Pumping Up the Volume
- Apple's Music Man

Newsweek

- Faith & Healing
- The Murky War in Iraq: Who is the Enemy?
- Led by Dean, Dems Fight for Black Voters
- Allan Sloan: Executives Behaving Badly

• E-MAIL THIS

• COMPLETE STORY

ADVERTISING ON MSNBC

- [Buy Life Insurance](#)
- [MSNBC Hot List](#)
- [Yellow Pages](#)
- [expedia.com](#)
- [Shopping](#)

UNFORTUNATELY, THE machines have “a fatal disadvantage,” says Rep. Rush Holt of New Jersey, who’s sponsoring legislation on the issue. “They’re unverifiable. When a voter votes, he or she has no way of knowing whether the vote is recorded.” After you punch the buttons to choose your candidates, you may get a final screen that reflects your choices—but there’s no way to tell that those choices are the ones that ultimately get reported in the final tally. You simply have to trust that the software inside the machine is doing its job.

It gets scarier. The best minds in the computer-security world contend that the voting terminals can’t be trusted. Listen, for example, to Avi Rubin, a computer-security expert and professor at Johns Hopkins University who was slipped a copy of Diebold’s source code earlier this year. After he and his students examined it, he concluded that the protections against fraud and tampering were strictly amateur hour. “Anyone in my basic security classes would have done better,” he says. The cryptography was weak and poorly implemented, and the smart-card system that supposedly increased security actually created new vulnerabilities. Rubin’s paper concluded that the Diebold system was “far below even the most minimal security standards.” Naturally, Diebold disagrees with Rubin. “We’re very confident of accuracy and security in our system,” says director of Diebold Election Systems Mark Radke.

After Rubin’s paper appeared, Maryland officials—who were about to drop \$57 million on Diebold devices—commissioned an outside firm to look at the problem. The resulting report confirmed many of Rubin’s findings and found that the machines did not meet the state’s security standards. However, the study also said that in practice some problems were mitigated, and others could be fixed, an attitude Rubin considers overly optimistic. “You’d have to start with a fresh design to make the devices secure,” he says.



Learn how voting technologies work

In the past few months, the computer- security community has been increasingly vocal on the problems of DRE terminals. "I think the risk [of a stolen election] is extremely high," says David Dill, a Stanford computer scientist. The devices are certified, scientists say, but the process focuses more on making sure that the machines don't break down than on testing computer code for Trojan horses and susceptibility to tampering. While there's no evidence that the political establishment actually wants vulnerable machines, the Internet is buzz-ing with conspiracy theories centering on these "black box" voting devices. (The biggest buzz focuses on the 2002 Georgia gubernatorial election, won by a Republican underdog whose win confounded pollsters.) Suspicions run even higher when people learn that some of those in charge of voting technology are themselves partisan. Walden O'Dell, the CEO of Diebold, is a major fund-raiser for the Bush re-election campaign who recently wrote to contributors that he was "committed to helping Ohio deliver its electoral votes for the president next year." (He later clarified that he wasn't talking about rigging the machines. Whew.)

To remedy the problem, technologists and allies are rallying around a scheme called verifiable voting. This supplements electronic voting systems with a print-out that affirms the voter's choices. The printout goes immediately into a secure lockbox. If there's a need for a recount, the paper ballots are tallied. It's not a perfect system, but it could keep the machines honest. If Representative Holt's proposed Voter Confidence Act is passed, verification will be the law of the land by the 2004 election, but prospects are dim, as the committee chairman, Bob Ney of Ohio, is against it.



Voting I: High-Tech, High Anxiety

- Audio: Steven Levy, NEWSWEEK senior editor and Congressman Rush Holt, Democratic, New Jersey, Author of proposed 'Voter Verification Act'
- Audio: Listen to the complete weekly On Air show

Critics of verifiable voting do have a point when they note that the printouts are susceptible to some of the same kinds of tricks once played with paper ballots. But there's a promise of more elegant solutions for electronic voting that are private,

verifiable and virtually tamperproof. Mathematician David Chaum has been working on an ingenious scheme based on encrypted receipts. But whatever we wind up using, it's time for politicians to start listening to the geeks. They start from the premise that democracy deserves no less than the best election technology possible, so that the vote of every citizen will count. Can anyone possibly argue with that?

© 2003 Newsweek, Inc.

MSNBC READER'S TOP 10

Would you recommend this story to other readers?

not at all **1** - **2** - **3** - **4** - **5** - **6** - **7** highly

[© BACK TO TOP ↗](#)

 NBC.COM

 Get MSN® 3 Months FREE!

MSNBC is optimized for
• Microsoft Internet Explorer
• Windows Media Player

• [MSNBC Terms, Conditions and Privacy © 2003](#)

[Cover](#) | [News](#) | [Business](#) | [Sports](#) | [Local News](#) | [Health](#) | [Technology & Science](#) | [Entertainment](#)
[Travel](#) | [TV News](#) | [Opinions](#) | [Weather](#) | [Comics](#)
[InfoCenter](#) | [Newsletters](#) | [Search](#) | [Help](#) | [News Tools](#) | [Jobs](#) | [Write Us](#) | [Terms & Conditions](#) | [Privacy](#)

MSN - More Useful Everyday

[MSN Home](#) | [My MSN](#) | [Hotmail](#) | [Search](#) | [Shopping](#) | [Money](#) | [People & Chat](#)

©2003 Microsoft Corporation. All rights reserved. [Terms of Use](#) [Advertise](#) [Truste Approved](#) [Privacy Statement](#) [GetNetWise](#)

Local

Swarthmore students refuse to comply with Diebold Co.

■ College faction claims public has right to know about memos illegally hacked from voting machine company.

By KRISTIN SMITH
ksmith@delcoimes.com

A group of Swarthmore College students are refusing to remove from their Web site a series of stolen internal company memos they say prove the company knowingly sold faulty voting machines to several states.

Taking a page out of Henry David Thoreau's book, the students say they are launching a system of "electronic civil disobedience."

The students allege the documents show the company, Diebold Election Systems of Ohio, knew there were security problems with many of their electronic voting machines.

The internal memos were hacked from Diebold's Web site in March by an unknown person and also contain information pertaining to some of the voting machines in Florida that were at the center of the 2000 presidential election controversy.

Those machines, however, were manufactured by Global Election Systems, a company Diebold purchased in January 2002.

The student group Why War?, a non-political organization, says it is their right and democratic duty to make the memos available for public inspection.

"It's so important to the public debate about these new election systems, we have to be truly confident our votes will be counted, especially after the Florida fiasco" said Andrew Main, 21, a junior at the college and Web master of Why War? "Anything that adds to this debate needs to be in the public arena."

The Why War? Web site, which operated by the students, was hosted by Swarthmore College. After receiving the cease-and-desist notice from the company, the college told the students they must take down the documents, although later indicated

they would work with the students if the proper legal procedures were followed.

Tom Crattenmaker, spokesperson for the liberal-arts college, said although no official position is being expressed, many of the faculty admire the students for their actions.

"I think I speak for most of us in the administration when I say we applaud their initiative and idealism," said Crattenmaker. "I respect them for acting on their consciences and I think most people would agree that fair elections and democracy are worthy causes."

A spokesperson for Diebold Inc., the parent company of Diebold Election Systems, said the company has been issuing the cease-and-desist orders to every person who puts up the stolen documents because they are copyrighted material.

When asked if there was any validity to the students' claims, Mike Jacobson said, "No, absolutely not ... our systems are accurate and secure."

Additionally, the vote counts have all been verified by state officials in every election in which the machines have been used, including the Florida 2000 presidential count, he said.

Jacobson went on to say that the internal documents being made public were probably deliberately corrupted or changed by anyone who had access to them.

The memos are incomplete," said Jacobson.

"They (people) see a memo or two and I think a lot of folks are making claims based on one or two memos and it's probably one piece of a long conversation e-mailed back and forth between Diebold folks."

66

Anything that adds to this debate needs to be in the public arena.

ANDREW MAIN, Swarthmore student

99

Main doesn't buy the company's assertion that the documents are taken out of context, but said he would welcome the opportunity to open a dialogue with Diebold.

"I'd be thrilled if Diebold would come in and enter the debate on those important issues, but at this point all they've had an interest in is suppressing discussion on the vulnerabilities revealed," he said.

The students, who are vowing to fight the issue until the finish, have been receiving legal advice from the Electronic Frontier Foundation, a group of lawyers in Calif. committed to preserving digital liberties.

The Swarthmore Coalition for the Digital Commons (SCDC), a group dedicated to preserving electronic free speech, bowed to the cease-and-desist order, but is investigating legal action against

the company.

"Diebold is essentially bluffing, they're trying to intimidate people into rolling over just like Swarthmore (College) did," said Luke Smith, a 19-year-old sophomore at the school and co-founder of SCDC. "We expect that if they force the issue, basically no matter what, if this case goes to court they lose. And we're confident that we're in the right legally."

Jacobson said it hasn't been decided yet if the company would take further action if the students continue to ignore the order. As for what Swarthmore College would do if the students become embroiled in a legal battle, Crattenmaker said it was a bridge they would cross when they came to it.

To view copies of the memos, visit www.why-war.com.

NEWS AND INFORMATION OFFICE

OCT 24 2003

Latest DMCA Takedown Victim: The Election Process

By [Ed Foster](#), Section [Columns](#)

Posted on Thu Oct 30th, 2003 at 09:19:07 AM PDT

"Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of the speech, or of the press ... except as needed to allow trademark and copyright holders complete power to control discussions about their brands."

Forgive my minor editing of the First Amendment, but I wanted to illustrate just where we are in the era of the DMCA (Digital Millennium Copyright Act). Nothing has made it clearer just how fundamentally the DMCA threatens our most basic rights than the current flap about electronic voting machines from Diebold, Inc.

Just as a capsule summary in case you've missed it, over the last several months there has been a rising tide of concern regarding the verifiability of electronic voting machines in general and the security, reliability, and integrity of Diebold's technology in particular. Adding fuel to the fire is the leaking of a large cache of internal Diebold documents and e-mails that have been circulating on the Internet. Critics pointed to memos that they said demonstrated Diebold's technology was buggy, badly tested, and vulnerable to backdoor manipulation. Some even claim to see evidence that outcomes of elections have already been influenced.

Perhaps not surprisingly, Diebold's first response was to begin cease-and-desist letterings to websites that had posted its internal memos, threatening to have those sites taken down under Section 512 of the DMCA. Section 512 provides a very big hammer to copyright holders because it requires Internet service providers to either quickly remove any allegedly infringing material they are hosting or face liability for the infringement themselves. If the ISP refuses, the copyright holder can go to the ISP's upstream provider and ask them to pull the plug. To protect themselves and their other customers, therefore, most ISPs will automatically and immediately take down their client's site upon receiving a 512 notification.

Diebold went the typical DMCA takedown one better, though. Not only did it go after the ISPs whose clients were posting the Diebold memos, it also began sending cease-and-desist letters to secondary sites that were reporting the controversy and merely contained hyperlinks to sites that were hosting the Diebold material. One such website and its ISP [refused to accede](#) to the DMCA takedown order and are being defended by the Electronic Frontier Foundation.

In other words, not only are you subject to DMCA takedown for what's on your own site, but you and your ISP are responsible for what might be on a site you link to. From a journalist's point of view

Menu

- [create account](#)
- [faq](#)
- [search](#)

Login

[Make a new account](#)

Username:

Password

[Login](#)

[Mail Password](#)

Related Links

- [refused to accede](#)
- [Blackbox Voting](#)
- [Why-War](#)
- [subscription page](#)
- [More on](#)
- [Also by Ed Foster](#)

this raises some interesting questions about how one can fairly report this story and provide readers with resources for making up their own minds without incurring Diebold's wrath.

When I asked Diebold spokesman Mike Jacobsen whether I could provide links to Diebold-targeted sites as Blackbox Voting or Why-War, he acknowledged I could but said that it was possible I could get a cease-and-desist notice. "I'm not saying we're going to do it, but you would be at risk for getting a letter," he said. "Anyone that's hosting a direct link to someone hosting those files, we want them to understand this is our stolen property and we want those links to be removed. Looking at it from a legal perspective, we were advised the DMCA was the best resource for getting that done. All we're really requesting that the links be removed from the site, although it does seem that the ISPs wind up taking down the whole site."

Of course, I'm probably going to have a long wait for my cease-and-desist letter, because Diebold's actions have backfired in a number of ways. A mushrooming number of sites are now mirroring the entire set of memos, and by claiming intellectual property rights to them, Diebold has given backhanded authentication to the material. But in using the DMCA to try to suppress the debate about its voting machines, Diebold has made another tactical error - it's closed off the discussion to all but its most virulent detractors. Academicians or journalists who might find evidence in the memos to debunk the more sensational claims about stolen elections are going to feel their hands are tied.

The Diebold controversy has raised a number of troubling questions that can only be answered by an unbiased, transparent examination of the facts. Trying to avoid that examination through questionable intellectual property will only leave a lingering cloud of suspicion hanging over the electoral process. And it proves yet again that the DMCA is in practice totally antithetical to everything Americans believe about how a democracy is supposed to work.

Post your comments about this column below or write me directly at Foster@gripe2ed.com. To receive this column every week in my free e-mail newsletter, please go to my subscription page and follow the instructions to opt-in for the EdFoster mailing list.

< [Napster 2.0's DRM problem](#) (1 comments)

View: Display: Sort:

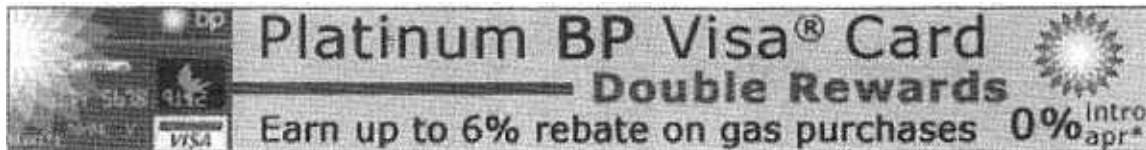
[Latest DMCA Takedown Victim: The Election Process](#) | 3 comments (3 topical, 0 editorial) | [Post A Comment](#)

What about search engines? (none / 0) (#1)
by Anonymous User on Thu Oct 30th, 2003 at 11:56:06 AM PDT

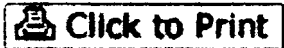
I'm curious whether Diebold has sent a cease and desist order to Google and the other search engines, which very likely contain links to the material in question.

are the search engines removing the links?

are their ISPs threatening to take them offline? THAT should raise some eyebrows!!



Powered by clickability



[SAVE THIS](#) | [EMAIL THIS](#) | [Close](#)

Worries grow over new voting machines' reliability, security

Touchscreen machines not the cure-all some expected

(AP) --Doubts about the trustworthiness of electronic voting machines are growing among election officials and computer scientists, complicating efforts to safeguard elections after the presidential stalemate of 2000.

With just over a year to go before the next presidential race, touchscreen voting machines don't seem like the cure-all some thought they would be. Skeptics fear they'll only produce more problems, from making recounts less reliable to giving computer hackers a chance to sabotage results.

"I'm deeply concerned about this whole idea of election integrity," said Warren Slocum, chief election officer in California's San Mateo County. His doubts were so grave that he delayed purchasing new voting machines and is sticking with the old ones for now.

He's not alone. While the Florida recount created momentum for revamping the way Americans vote, slow progress on funding and federal oversight means few people will see changes when they cast ballots next week. And new doubts could further slow things.

In Florida's Broward County -- scene of a Bush-Gore recount of punch-card ballots -- officials spent \$17.2 million on new touchscreen equipment. Lately, they've expressed doubts about the machines' accuracy, and have discussed purchasing an older technology for 1,000 more machines they need.

The concerns focus on

- Voter confidence: Since most touchscreen machines don't create a separate paper receipt, or ballot, voters can't be sure the machine accurately recorded their choice.

- **Recounts:** Without a separate receipt, election officials can't conduct a reliable recount but can only return to the computer's tally.
- **Election fraud:** Some worry the touchscreen machines aren't secure enough and allow hackers to potentially get in and manipulate results.

"The computer science community has pretty much rallied against electronic voting," said Stephen Ansolabehere, a voting expert at the Massachusetts Institute of Technology. "A disproportionate number of computer scientists who have weighed in on this issue are opposed to it."

Other doubters say the solution would be "voter verifiable paper trails" -- a paper receipt that voters can see to be confident of their choice, that can then be securely stored, and that election officials can rely on for recounts.

Federal election-reform legislation passed in 2002 aims to upgrade voting systems that rely on punch-card ballots or lever machines, and to improve voter registration, voter education and poll worker training

States upgrading their equipment are looking at two systems: electronic machines, with voters making their choice by touchscreens similar to ATMs; and older optical scan machines, with voters using pen and paper to darken ovals, similar to standardized tests.

Still, North Dakota changed its plan to give officials the flexibility to go with touchscreens or optical scan machines. And the National Association of Secretaries of State held off from embracing touchscreens at its summer meeting, pending further studies.

"This is too important to just sort of slam through," said William Gardner, New Hampshire's secretary of state. In Congress, Rep. Rush Holt, D-New Jersey, has introduced a bill that would require that all voting machines create a paper trail.

Critics mistaken

Computer manufacturers and many election officials say the critics are mistaken. They insist that security is solid and machines records are examinable. They also say the sought-after improvements will create other problems, such as malfunctioning machines and violating the integrity of a voters' privacy.

Slocum figures that only about a half-dozen of California's county election commissioners share his concerns.

The complaints echo those that came up when lever machines were introduced in the 1920s, and again when punch cards came on the scene, said Doug Lewis, an expert at The Election Center in Houston Texas.

"We were going to find that elections were manipulated wildly and regularly. Yet there was never any proof that that happened anywhere in America," Lewis said.

David Bear, a spokesman for Diebold Election Systems Inc., one of the larger voting machine makers, said "the fact of the matter is, there's empirical data to show that not only is electronic voting secure and accurate, but voters embrace it and enjoy the experience of voting that way."

This week, a federal appeals court in California threw out a lawsuit that challenged computerized voting without paper trails, finding that no voting system can eliminate all electoral fraud.


That didn't satisfy doubters.

John Rodstrom Jr., a Broward County, Florida, commissioner said local officials there wanted to upgrade to optical scan machines, but were pressured into buying more than 5,000 touchscreens.

"We were forced by the Legislature to be a trailblazer," he said. "The vendors ... they're going to tell you it's perfect and wonderful. (But) there are a lot of issues out there that haven't been answered. It's a scary thing."

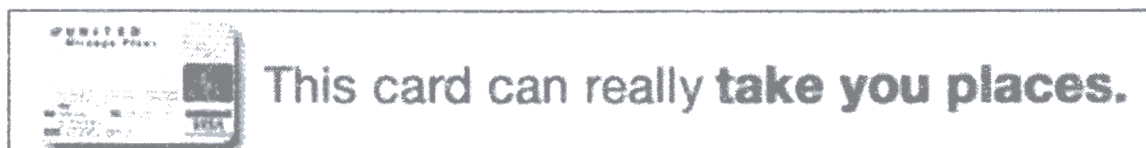
Find this article at:

<http://www.cnn.com/2003/ALLPOLITICS/10/30/elec04.election.worries>

 **Click to Print**

[SAVE THIS](#) | [EMAIL THIS](#) | [Close](#)

Check the box to include the list of links referenced in the article.



Why War?

why-war.com

Targeting Diebold with Electronic Civil Disobedience

Our Positions

(Oct. 21)

(Oct. 23)

Prepared by STAFF for *Why War?*

Why are these memos controversial? Read the excerpts and see for yourself, then read the campaign update for the latest news.

Electronic Civil Disobedience

How to get the files: Note that the location of the documents may change, but this page will always have the current links. In case Diebold takes down this page, bookmark cultcom.com/mirror.html or web.umn.edu/~gabriels/diebold.html. You must currently copy and paste the URL because Diebold has attacked our right to deep-link to the memos.

Diebold Elections Systems

(also read and)

Note: Can't highlight the text? [Click here.](#)

- **Browse** the documents: <http://chroot.net/s/lists/>,
<http://www.sims.berkeley.edu/~ping/diebold/lists.html>
- **Search** the documents: <http://diebold.f-451.net/search/search.php>
- **BitTorrent:** <http://cscott.net/Activism/lists.tgz.torrent>
- **EDonkey/Overnet:**
[\[ed2k://file|list.tar.bz2|7762005|c53855d1c5da1fec2da1548905bc689f|/\]](http://ed2k://file|list.tar.bz2|7762005|c53855d1c5da1fec2da1548905bc689f|/)
- **Freenet:**
CHK@sgOjWAY4g-0bf0m5biyqnEzWloENAwI,OXw8OfHPfsmLd068BtICKg/lists.tgz
CHK@fsatUAqLqJP91UTrCoReT3qciVYNawI,whenOQbgnMLSo84zg1~aA/lists.tar.bz2
- **Newsgroup postings:** Help us do this
- **Archived file** (tarred and gzipped):
<http://eddie.ratm.net/johnkimble/lists/lists.tgz>
<http://www3.telus.net/swix/list.tar.bz2> (*checksum, sig*)
On a Windows PC, use WinZip or WinRAR; on a Mac just double-click the file
- **.edu hosts** of the documents (*both archived and full-text*):
 - **Swarthmore College** (*takedown request received*)
 - **Swarthmore College** (*takedown request received*)
 - **Univ. of Southern California** <http://www-scf.usc.edu/~kanawi/lists.tgz>
 - **Massachusetts Institute of Technology** (*takedown request received*)
 - **Massachusetts Institute of Technology** (*takedown request received*)
 - **Massachusetts Institute of Technology**

Articles About the Controversy

Newsweek:

Associated Press:

Wired News:

Associated Press:

Truthout:

Independent:

Baltimore Sun:

Seattle Times:

New York Times:

Salon:

Scoop:

Cleveland Plain Dealer:

Wired News:

San Diego Union-Tribune:

MSNBC:

Scoop:

- <http://web.mit.edu/chrisk/www/diebold/list.tar.bz2>
- **Purdue University** (*takedown request received*)
 - **Univ. of Texas–Pan American** (*takedown request received*)
 - **Amherst College** (*takedown request received*)
 - **Hampshire College** <http://stout.hampshire.edu/~pks03/list.tar.bz2>
 - **Rochester Institute of Technology**
<http://www.cs.rit.edu/~cmm5533/diebold/lists.tgz>
 - **Rochester Institute of Technology** <http://libre.rh.rit.edu/lists.tgz>
 - **Rochester Institute of Technology** <http://rancor.rh.rit.edu/>
 - **Rochester Institute of Technology** <http://www.rit.edu/~tjd3307/lists.tar.bz2>
 - **Univ. of Evansville** <http://csserver.evansville.edu/~sc87/diebold/>
 - **Boston University** <http://cs-people.bu.edu/chrisn1/diebold-memos.tgz>
 - **Carnegie Mellon University** <http://www.cs.cmu.edu/~matth/lists>
 - **Carnegie Mellon University**
<http://www.andrew.cmu.edu/~dcheng/diebold/lists.tgz>
 - **Carnegie Mellon University** <http://andrew.cmu.edu/~apapadop/lists.tgz>
 - **Univ. of Missouri–Rolla** (*takedown request received*)
 - **Indiana University** (*takedown request received*)
 - **Harvard University** (*takedown request received*)
 - **Univ. of California–Berkeley** (*takedown request received*)
 - **Univ. of California–Berkeley** <http://sims.berkeley.edu/~parkert/misc/lists.tgz>
 - **Univ. of California–Berkeley** <http://sims.berkeley.edu/~ping/diebold>
 - **Univ. of California–Berkeley** <http://sims.berkeley.edu/~savage/lists.tgz>
 - **Duke University** <http://www.cs.duke.edu/~justin/archive/diebold.html>
 - **Univ. of North Carolina at Chapel Hill** <http://www.unc.edu/~cjp2/lists.tgz>
 - **North Carolina State University** <http://www4.ncsu.edu/~jgkimbro/diebold.html>
 - **Univ. of Pennsylvania** <http://www.seas.upenn.edu/~dmargoli/lists.tgz>
 - **Grinnell College** <http://www.math.grinnell.edu/~laiu/lists.tgz>
 - **Grinnell College** <http://web.grinnell.edu/individuals/laiu/lists.tgz>
 - **Grinnell College**
<http://www.math.grinnell.edu/~lyonavra/diebold/lists/index.html>
 - **Wright State University** <http://www.wright.edu/~stine.8/politics/list.tar.bz2>
 - **Univ. of Maryland–College Park**
<http://www.glue.umd.edu/~chsimps/diebold/lists.tgz>
 - **Univ. of Chicago** <http://home.uchicago.edu/~mhwang/lists.tgz>
 - **Univ. of Chicago** <http://home.uchicago.edu/~yitzhak/list.tar.bz2>
 - **Univ. of Chicago** <http://people.cs.uchicago.edu/~ryochiji/>
 - **Bentley College** http://web.bentley.edu/students/h/heap_aust/lists.tgz
 - **Penn State University** <http://www.personal.psu.edu/~mjo168/lists.tgz>
 - **Penn State University**
<http://www.personal.psu.edu/users/b/j/bje128/diebold.html>
 - **Princeton University** <http://www.princeton.edu/~kleinman/diebold.html>
 - **Princeton University** <http://www.princeton.edu/~bcattle/diebold.html>
 - **Princeton University** <http://www.princeton.edu/~cpence/diebold-lists.tgz>
 - **Michigan State University** <http://www.msu.edu/~justmanj/lists.tgz>
 - **Iowa State University** <http://www2.iastate.edu/~daoist/diebold-lists.tgz>
 - **University of Washington–Tacoma**
<http://faculty.washington.edu/dmclane/lists.tgz>
 - **Johns Hopkins University** <http://myweb.jhu.edu/bananas/diebold-lists.tgz>
 - **Kent State University** <http://www.personal.kent.edu/~sfidel/lists.tgz>
 - **Kent State University** <http://www.personal.kent.edu/~bmconah/lists.tgz>
 - **Rose-Hulman Institute of Technology** <http://www.rose-hulman.edu/~gordonmw/lists.tgz>

- **Yale University**
http://yale128036068211.student.yale.edu/~andrew/diebold/lists.tgz
- **Bronx High School of Science** http://www.bxscience.edu/~dauriaa/lists.tgz
- **Dartmouth College** http://www.cs.dartmouth.edu/~apd/lists.tgz
- **Georgetown University** http://saxa.georgetown.edu/lists.tgz
- **Illinois Mathematics and Science Academy**
http://alumni.imsa.edu/~hangman/lists.tgz
- **Lafayette College** http://www.cs.lafayette.edu/~ahmedf/archive/lists.tgz
- **Univ. of Illinois–Urbana-Champaign** http://www.cen.uiuc.edu/~badr/lists.tgz
- **Univ. of Virginia** http://www.people.virginia.edu/~ajs6f/lists.tgz
- **Univ. of Wisconsin–Milwaukee** http://www.uwm.edu/~cmerkel/lists.tgz
- **Univ. of Wisconsin–Milwaukee** http://www.uwm.edu/~puissan2/
- **Georgia Southern University**
http://www.georgiasouthern.edu/~jtwyford/list/list.tar.bz2
- **Middle Tennessee State University** http://www.mtsu.edu/~cow2a/lists.tgz
- **Ohio State University** http://www.cis.ohio-state.edu/~wangje/lists.tgz
- **Stanford University** http://www.stanford.edu/~drumz/lists.tgz
- **Stanford University** http://www.stanford.edu/~ssavage/lists.tgz
- **Stanford University** http://www.stanford.edu/~fire/lists.tar.tar
- **Stevens Institute of Technology** http://attila.stevens-tech.edu/~pgengler/lists.tar.bz2
- **Rensselaer Polytechnic Institute** http://www.cs.rpi.edu/~paulj/lists.tgz

Please e-mail ecd-info@why-war.com if you are willing to publicly mirror the files (either the archive or the full text); contact web@why-war.com to report broken links. We are especially interested in hearing from individuals at other educational institutions. Please note that due to overwhelming volume, we will attempt to keep the links up to date but may not respond to specific e-mails of this type. Members of the press can contact media@why-war.com

Campaign Update

Day Thirteen, Nov. 2: Stephen Ansolabahere, a voting analyst at MIT, is quoted in an *Associated Press* story as saying:

The computer science community has pretty much rallied against electronic voting. A disproportionate number of computer scientists who have weighed in on this issue are opposed to it.

This is certainly borne out by this campaign — we now have 50 schools involved, including recent additions from Stanford, Grinnell, Princeton, Georgetown, Chicago, Rensselaer and two high schools. The mirrors are staying well ahead of Diebold's takedown requests.

Why War? will soon be moving this information to a new website in order to allow the electronic civil disobedience campaign to prosper under its own momentum, and in acknowledgement of the vast number of students beyond our own group now engaged in this activity. Check back here for more information in the near future.

Day Nine, Oct. 29: The following is a statement by Why War? member Micah White, a senior in philosophy and a minor in interpretation theory at Swarthmore College in Swarthmore, Pa.:

Diebold can't win! Each takedown request is simply met with more mirrors. We are willing and able to continue this campaign until the 2004 presidential elections. We will not allow Diebold's faulty voting machines to replace democracy.

Why War? has now received a second takedown request (*first letter, second letter*). Diebold's use of the DMCA is absurd and their actions are irrelevant. Nearly 100,000 people have now read this website. We estimate that at least 30,000 people have downloaded the entire collection of 13,000 memos directly from just three of the mirrors above. The memos are on peer-to-peer file trading systems. They are in Freenet.

Diebold is, by its corporate nature, providing proof for the suspicions of millions of people world wide who are now beginning to hear about this controversy. Diebold, we will not stop until there is an open examination of your misdeeds. (Will they put that line in their next takedown request?)

What will Diebold do when they cannot stop the movement from posting their memos? How will they retaliate?

The response thus far has been amazing. If Why War? doesn't respond immediately to your e-mail we apologize, but we do need your mirrors. Directions are available.

Day Eight, Oct. 28: Amherst and MIT have received takedown requests (*copy of MIT takedown request*). New mirrors are now up at UNC, Duke, Berkeley, NCSU and U Penn.

Diebold has publicly admitted that leaked memos do not meet DMCA standards for copyright infringement. In the *Associated Press* article, a Diebold representative declares:

... the fact that the company sent the cease-and-desist letters does not mean the documents are authentic — or give credence to advocates who claim lax Diebold security could allow hackers to rig machines.

"We're cautioning anyone from drawing wrong or incomplete conclusions about any of those documents or files purporting to be authentic," Jacobsen said.

Ernest Miller explains that the DMCA requires that documents be authentic; if the documents

aren't authentic, it isn't copyright infringement. Our position is that even if the memos *are* authentic (which we believe they are, or Diebold would be pursuing a libel campaign), they are not copyright infringement as they are covered under DMCA fair use guidelines.

Since some of you have been asking, yes, Swarthmore College is still enforcing its policy of cutting off network access to students who link to information about the memos (or the memos themselves). There have been many discussions of this absurd policy — see, for instance, *LawMeme's* analysis — and we appreciate the letters that are being sent to Dean Gross and *The Phoenix* (e.g. Seth Finkelstein's). We hope that by expanding to other colleges and universities we can broaden the campaign while minimizing the impact of our own institution's refusal to take a stand. (If other educational institutions encounter such policies, this script may be of help.)

Day Seven, Oct. 27: The movement is winning. The story is spreading (*Associated Press*). Diebold's actions are being thrust into the light. How long can they pursue the sepression of evidence that links them directly to election fraud? Every lawsuit is simply another admission of guilt. Thus, we are pleased to announce that students at Indiana University, Harvard, and Berkeley have now joined this campaign against Diebold.

Today Andrea Foster authored an excellent article about this battle in the *Chronicle for Higher Education*. She writes:

[A spokesperson] said Diebold will continue to send copyright-infringement notices to Internet service providers that host the company documents, including the four other institutions — the Massachusetts Institute of Technology, Purdue University, the University of Southern California, and the University of Texas–Pan American. The materials were first obtained by Bev Harris, who is writing a book about modern-day ballot-tampering. According to published accounts, she found the materials on an unprotected Web site while doing a Google search.

Why War? asks that the movement call their bluff. Together, we can create a permanent, public, and *easily accessible* location for these memos. Those unable to mirror should use their talents in other ways. We need people to be deep-reading these memos and sharing exerpts. Others need to be calling their election officials and demanding that they address your concerns (one request could be this bill). And, of course, others need to be sharing with us all how to short sell Diebold's stock so that when its price decreases the movement will prosper. Investors, now is your chance to join the struggle.

Day Six, Oct. 26: Three additional schools have been added to the list. There are now eleven .edu mirrors.

Day Five, Oct. 25: Students from four more universities, along with a second mirror at MIT, have joined the campaign.

Day Four, Oct. 24: Students from four American universities have joined the civil disobedience: MIT, USC, Purdue and the University of Texas–Pan American. Check out Black Box Voting for a startling expose on Diebold's connection to the debacle in Florida. This is from the individual who broke the whole story about Diebold.

A visitor wrote an e-mail of support and noted:

While doing some research about electronic voting and the Diebold machines in particular, I came across this story alleging widespread vote skimming by Diebold systems in the recent California Recall election.

I think these allegations merit wider distribution and further investigation. It is important to note that these allegations include Diebold optical scan results, allowing for the possibility of a manual recount to substantiate or refute the claims made.

More information is available [here](#).

Day Three, Oct. 23: Just as the civil disobedience campaign is starting to break into the mainstream press, Swarthmore College has decided to further their suppression of the Diebold memos. College policy is now that *any* links to why-war.com with the intention of providing information about Diebold will result in termination of that student's Internet connection. Therefore, it is now a punishable offense for any Swarthmore student to link to the page you are now reading! Because of the wide support that this issue is receiving from the students, faculty, and staff of Swarthmore — including many e-mails of support and a positive editorial in the campus newspaper — we are confused by Swarthmore's refusal to take a pro-democracy stance on this issue. Swarthmore's latest repression turns this act of civil disobedience into one protecting both fair elections and free speech — the ability to link to websites.

We encourage you to send letters voicing your opinions directly to Swarthmore's student newspaper, *The Phoenix* (phoenix_letters@swarthmore.edu). You may want to reference some of the excerpts we've selected from the college's literature (*see below*).

The good news is that the civil disobedience continues and we are receiving massive amounts of

support from both the press and the Internet-at-large. This is in addition to reports that have already appeared in Slashdot, *Wired News*, *Philadelphia Daily News*, Infoshop, *The Inquirer* and elsewhere.

We thought it might be informative to reference Swarthmore's own stated mission. The following are quotes from their "Mission Statement":

Foremost among these principles is the individual's responsibility for seeking and applying truth and for testing whatever truth one believes one has found.

A college draws strength from tradition and energy from the necessity of change. Its purposes and policies must respond to new conditions and new demands. By being open to change, Swarthmore tries to provide for its students, by means appropriate to the times, the standard of excellence it has sought to maintain from its founding.

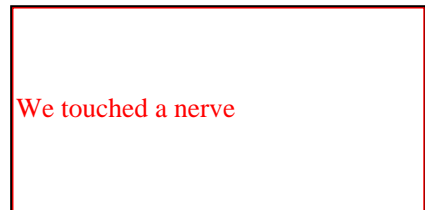
The purpose of Swarthmore College is to make its students more valuable human beings and more useful members of society.

The following quotes are from the admissions website:

The purpose of Swarthmore's liberal arts curriculum is to help students fulfill their responsibilities as citizens and grow into cultured and versatile individuals.

Swarthmore is about making a difference in the world. There's a real emphasis on making things better—not just identifying problems or theorizing about solutions, but actually rolling up your sleeves and improving some corner of your community.

Day Two, Oct. 22: Today Why War? and the Swarthmore Coalition for the Digital Commons held a public meeting with Dean Bob Gross of Swarthmore College. Overnight, word had spread of this action and Gross had received over 250 emails of support from individuals throughout the world including "tech celebrities" and Swarthmore alumni.



why-war.com

Demonstrating massive concern about fair elections, over 42,000 people visited Why War? to read

Diebold's memos.

Swarthmore College, unfortunately, is not willing to take a strong stand against Diebold, and is systematically disabling the network access of any student who hosts the files. "We can't get out in front in this fight against Diebold," Gross said during the meeting with over fifty students, staff, and faculty. Gross, apparently, did not see that by taking an active stance against Why War's actions Swarthmore was aiding Diebold's suppression.

Although Why War? acknowledges Swarthmore's position, we will continue to explain the importance of this issue to the administration. We had hoped that an institution once praised for allegiance to the pursuit of truth would have taken a more forceful stance in defense of information. Under the Digital Millennium Copyright Act, the college would be under *no liability* after informing a student that s/he should not be hosting the file. Yet Swarthmore is choosing to act counter to the spirit of both its traditions and rules, the latter of which requires that students be given three days to take down work challenged as an infringement of copyright. There is no provision under either the DMCA or Swarthmore's own rules to allow for shutting down a student's network access when no challenge has been made against that specific student. Why War? is deeply distressed by Swarthmore's inability, or unwillingness, to understand that the magnitude of this situation: a fair presidential election!

After consultation with SCDC, the two groups have decided to work independently of each other. SCDC will now issue statements on their website. Why War? will continue to provide access to the memos by listing mirrors provided by individuals worldwide.

If you would like to join this campaign of electronic civil disobedience by hosting the memos please e-mail ecd-info@why-war.com. For those unable to host the documents, we encourage you to send letters expressing your disappointment about Swarthmore's lack of principle directly to the college newspaper, at phoenix_letters@swarthmore.edu (and please cc your letters to us).

Representatives of the media should contact media@why-war.com.

Why War? believes that what we are doing is *legal*; though we see it as an issue of electronic civil disobedience we believe it is Diebold which is abusing copyright law in an attempt to shut down free speech and the democratic process. The four criteria of "fair use" copyright law are the purpose of the use, the nature of the copyrighted work, the substantiality of the portion used and the effect of the use upon the potential market of the copyrighted work. We believe the publication of these documents is integral to the function of the democratic process. The memoranda themselves are not marketable products, and in this case we believe the nature of the work, which threatens elections occurring in 37 states, outweighs the need to selectively excerpt

portions of the documents. If there is anything the American people have a right to know, it is how their votes are being counted.

Read our earlier press release.

Excerpts from the Diebold Documents

“Elections are not rocket science. Why is it so hard to get things right! I have never been at any other company that has been so miss [sic] managed.” [source:

<http://chroot.net/s/lists/announce.w3archive/200110/msg00002.html>]

In response to a question about a presentation in El Paso County, Colorado: “For a demonstration I suggest you fake it. Program 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 demo.” [source:

<http://chroot.net/s/lists/support.w3archive/199903/msg00098.html>]

“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 then make excuses at delivery time when these products and services do not meet expectations.” [source:

<http://chroot.net/s/lists/announce.w3archive/200110/msg00001.html>]



dieboldes.com

Diebold voting machines are used in 37 states and provide zero security against election fraud.

“I feel that over the next year, if the current management team stays in place, the Global [Election Management System] working environment will continue to be a chaotic mess. Global management has and will be doing the best to keep their jobs at the expense of employees.

Unrealistic goals will be placed on current employees, they will fail to achieve them. If Diebold wants to keep things the same for the time being, this will only compound an already

dysfunctional company. Due to the lack of leadership, vision, and self-preserving nature of the current management, the future growth of this company will continue to stagnate until change comes.” [source: <http://chroot.net/s/lists/announce.w3archive/200112/msg00007.html>]

“[T]he bugzilla historic data recovery process is complete. Some bugs were irrecoverably lost and they will have to be re-found and re-submitted, but overall the loss was relatively minor.”

[source: <http://chroot.net/s/lists/support.w3archive/200207/msg00090.html>]

“28 of 114 or about 1 in 4 precincts called in this AM with either memory card issues "please re-insert", units that wouldn't take ballots - even after recycling power, or units that needed to be recycled. We returned 7 memory cards, 4 of which we didn't need to, but they were far enough away that we didn't know what we'd find when we got there (bad rover communication).”

[source: <http://chroot.net/s/lists/support.w3archive/200003/msg00034.html>]

“If voting could really change things, it would be illegal.” [source:

<http://chroot.net/s/lists/support.w3archive/200009/msg00109.html>]

“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. Will someone please explain this so that I have the information to give the auditor instead of standing here "looking dumb".” [source:

<http://chroot.net/s/lists/support.w3archive/200101/msg00068.html>]

“[...] while reading some of Paranoid Bev's scribbling.” [source:

<http://chroot.net/s/lists/support.w3archive/200302/msg00069.html>]

“Johnson County, KS will be doing Central Count for their mail in ballots. They will also be processing these ballots in advance of the closing of polls on election day. They would like to log into the Audit Log an entry for Previewing any Election Total Reports. They need this, to prove to the media, as well as, any candidates & lawyers, that they did not view or print any Election Results before the Polls closed. *However, if there is a way that we can disable the reporting functionality, that would be even better.*” [source:

<http://chroot.net/s/lists/rcr.w3archive/200202/msg00051.html>] (emphasis added)

“4K Smart cards which had never been previously programmed are being recognized by the Card Manager as manager cards. When a virgin card from CardLogix is inserted into a Spyrus (have tried CM-0-2-9 and CM-1-1-1) the prompt "Upgrade Mgr Card?" is displayed. Pressing the

ENTER key creates a valid manager card. This happens in Admin mode and Election mode.

[source: <http://chroot.net/s/lists/bugtrack.w3archive/200201/msg00025.html>]

Read the latest electronic civil disobedience campaign update.