IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,
Plaintiff

DECLARATION OF JOANNE LUKACHER

v

Case No. 06-CV-0263 (GLS)

NEW YORK STATE BOARD OF ELECTIONS; PETER KOSINSKI and STANLEY L. ZALEN, Co-Executive Directors of the New York State Board of Elections, in their official capacities; and, STATE OF NEW YORK,
Defendants

Pursuant to 28 U.S.C. sec 1746, **JOANNE LUKACHER**, declares as follows:

1.I am an executive member of Northeast Citizens for Responsible Media (Re-Media), www.re-media.org and am authorized to seek leave to appear as *amius curiae* on behalf of Re-Media.

2.Re-Media is a grass roots media reform organization founded in the Hudson Valley, extending throughout the northeast parts of New York. The organization was formed in response to the recognition that our democracy has been precariously threatened by the deliberate restriction of ideas and information, now in the hands of a few corporations who control what was to be a free press in service to the people. It is our goal to bring awareness of our essential need and right to responsible media -- media which is independent, investigative and truth

seeking. Our organization seeks to bring to our communities essential information, not otherwise being addressed by the main stream media, through forums, screenings of documentaries and over the internet, providing sources of alternative information and independent media.

3.Recently we have focused on the issue of democratic elections and voting machines in New York because citizens' ability to vote freely and know that their votes were counted as cast is fundamental to the continuation of our democracy.

4.This year we held a number of forums on the issue, bringing experts to the New York region to educate and inform citizens of the dangers of computerized voting systems and the need for people to be able to retain control over their elections through a transparent, accountable electoral process.

5.We have published numerous well-researched papers on the subject, available at www.opednews.com, www.freepress.org and the Brad Blog, focusing on the problems computerized voting has caused and the need for transparent, observable elections.

6.We have held screenings of the various election integrity documentaries that have exposed the massive problems across the country since states began purchasing computerized voting systems only to witness the disenfranchisement of their citizens.

7.We have organized letter writing campaigns to our legislators, the State Board of Elections, our county election commissioner and the Governor, but do not believe we are being heard or worse, are being ignored.

8.We are deeply concerned about our democracy and the consequences for its continuation should computers be installed in New York preventing human beings from being able to observe the processing and counting of our votes.

9.We understand that democracy requires vigilance and that checks and balances are essential. Computerized voting systems remove citizens from the process of their elections, forcing us to blindly trust those we are responsible for electing and holding accountable. We cannot trust what we cannot see and checks and balances, fundamental to our democratic roots, requires that we never surrender our civil responsibility by trusting the government to inform us of how they were elected or reelected.

10.We understand the United States is urging that New York purchase these machines and we are opposed to a voting system that relies on computerized machines which not only conceal the very information citizens must be able to observe, but have been repeatedly shown to be so unreliable that they can be manipulated without detection.

11.We are opposed to being disenfranchised by computerized voting systems which dozens of independent studies have revealed to be so vulnerable to manipulation as to be capable of changing the outcome of an entire election. [1] Below is just a sampling from some of the independent reports exposing the ways

[1] http://www.guvwurld.org/Election%20Reform/Rady%20Ananda%20-%20Tech%20Reports%20-%2012-07.pdf
http://tinyurl.com/2okz67

in which computers stand between citizens and their right to fair, reliable and trustworthy elections.

12. **July 2007 - California's Secretary of State Released the Findings of the Most Extensive Top-to-bottom Independent Testing[2] of DREs and Optical Scanners Used Throughout the Nation Confirming the Voting Systems Offered in the U.S. Are Insecure, Unreliable and Inaccessible.**

The researchers in California found all the computerized voting systems tested lacked effective safeguards to prevent tampering and fraud concluding that:

> *Virtually every important software security mechanism is vulnerable to circumvention .....All of the attacks described in this report can be carried out without any knowledge of the source code*[3].

13. Every voting system tested by the California Secretary of State was susceptible to computer viruses that could infect any of the systems, spread between voting machines and steal votes on the infected machines, changing the outcome of the elections. The expert reviewers demonstrated:

> *that the security mechanisms provided for all systems analyzed were* ***inadequate to ensure accuracy and integrity of the election results*** *and of the systems that provide those results.*[4]
>
> ***An attack could plausibly be accomplished by a single skilled individual with temporary access to a single voting machine****. The damage could be extensive- malicious code could spread to every voting machine in polling places to county election servers.*[5]

---

[2] http://www.sos.ca.gov/elections/elections_vsr.htm

[3] http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf

[4] http://www.sos.ca.gov/elections/voting_systems/ttbr/red_overview.pdf

[5] http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf

14. The California Secretary of State's Report confirmed that all of the state's Hart, Diebold and Sequoia DRE and OpScan voting systems can be hacked in a variety of ways. The researchers had corroborated previous studies revealing the hack which has the voter verified paper audit trail (VVPAT) print out one thing and the DRE electronic total reflect something else, thus rendering the VVPAT worthless. The researchers also demonstrated the computers' ability to detect election mode, thus enabling the pre-election testing to appear correct, while the actual election has been manipulated!

15. ES&S had failed to provide requested information to the California Secretary of State's office on time and hence their equipment was not included in the top-to-bottom review released this past August. The Secretary of State has now completed the top-to-bottom review for ES&S's systems[6] and has found similar flaws in ES&S's voting systems; flaws "that could leave it vulnerable to fraud or electronic hacking. [7]

16**. July 2007 - Florida's Department of State released its report[8] corroborating once again that Diebold's Optical Scanner remains vulnerable to being hacked without detection.**

---

[6] http://www.sos.ca.gov/elections/voting_systems/inka_vote_plus_public_red_team_report.pdf

[7] L.A. County Voting System Flawed, Daily News, Los Angeles, November 24, 2007

[8] http://election.dos.state.fl.us/pdf/SAITreport.pdf

Diebold's Optical Scanners remain seriously flawed and uncorrected. As reported by the Philadelphia Inquirer [95] on August 1, 2007:

> *someone with only brief access to a machine could replace a memory card with one preprogrammed to read one candidate's votes as counting for another, essentially switching the candidates and showing the loser winning in that precinct.*
>
> *The attack can be carried out with a reasonably low probability of detection assuming that audits with paper ballots are infrequent.*

According to a story in the Miami Herald[10]:

> *the Florida Secretary of State's office has conducted an elections study that confirmed Tuesday what a maverick voting chief discovered nearly two years ago:* ***Insider computer hackers can change votes without a trace on Diebold optical-scan machines.***[11] (emphasis supplied)

17. February 2007 – Princeton University professor hacks Sequoia DRE in seconds. Like Diebold's DRE machines before them[12] Sequoia's DREs weres able to be hacked in a matter of seconds by a Princeton University professor who stated the systems could be "easily...rigged to throw an election."[13]

> *We can take a version of Sequoia's software program and modify it to do something different --- like appear to count votes, but really move them from one candidate to another. And it can be programmed to do that only on Tuesdays in November, and at any other time. You can't detect it.*

---

[9] http://www.philly.com/inquirer/world_us/8846277.html

[10] http://mparent7777-2.blogspot.com/2007/08/state-fla-voting-machines-can-be-hacked.html

[11] http://www.bradblog.com/?p=4900

[12] http://www.salon.com/opinion/feature/2006/09/13/diebold/

[13] SEQUOIA TOUCH-SCREEN VOTING MACHINES HACKED, FOUND VULNERABLE TO VOTE-FLIPPING BY PRINCETON UNIVERSITY! http://www.bradblog.com/?p=4141

18. **December 2006 - Report of the National Institute of Standards and Technology (NIST)[14], technical advisors to the Federal Government, found DREs: "are vulnerable to errors and fraud and cannot be made secure":**

> *The DRE provides no independent capability to detect whether fraud has not caused errors in the records..... a single... programmer ...could rig an entire statewide election.*

The NIST research staff further stated that they,

> *do not know how to write testable requirements to satisfy that the software in a DRE is correct.*

19. **October 2006 – University of Connecticut finds Diebold's Optical Scanner can be manipulated to invalidate the results of an election process**.

The Report[15] further revealed that vote tabulations could be corrupted and lay dormant until election day, thus avoiding detection through pre-election tests. Avi Rubin, Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University, who led the first group of computer scientists examining Diebold's software in the Rubin Report, described the report from the University of Connecticut this way:

> *Reading this report was a hair raising experience for me. Diebold has clearly not learned any of the lessons from our 2003 report, and it is startling to see that their optical scan ballot counter is as vulnerable to tampering, vote rigging, and incorrect tabulation as the DRE.* [16]

---

[14] http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf,

[15] http://voter.engr.uconn.edu/voter/Reports.html

[16] http://avi-rubin.blogspot.com/2006/10/uconn-voter-center-report-diebold-av-os.html

20. **The Report of California's Voting System Technical Assessment and Advisory Board[17] found that certain types of hacks on the Diebold Optical Scanners can never be detected unless the ballots are counted by hand**.

The 2006 California report commissioned by California's Secretary of State, warned:

> *...successful attacks can only be detected by examining the paper ballots. There would be no way to know that any of these attacks occurred; the canvass procedure would not detect any anomalies, and would just produce incorrect results. The only way to detect and correct the problem would be by recount of the original paper ballots.*

21. **Government Accountability Office's Reports have on two occasions expressed concern that the problems with electronic voting systems are so pervasively problematic they "could damage the integrity of ballots, votes and voting-system software by allowing unauthorized modifications**."[18]

In the more recent study by the Government Accountability Office (GAO), released March 7, 2007[19], the GAO Information Technology Architecture and Systems Director, Randolph C. Hite, testified that electronic voting systems can break an election!

> *"[E]lectronic voting systems are an undeniably critical link in the overall election chain. While this link alone cannot make an election, it can break one. The problems that some jurisdictions have experienced and the serious concerns that have surfaced highlight the potential for continuing difficulties in upcoming national elections if these challenges are not effectively addressed.*

---

[17] http://ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf, (confirming the findings of the Hursti Hack, Black Box Report Security Alert: July 4, 2005 Critical Security Issues with Diebold Optical Scan Design (1.94w), 2005, http://www.blackboxvoting.org/BBVtsxstudy.pdf)

[18] October 2005 Report http://www.gao.gov/new.items/d05956.pdf

[19] October 2007 Report http://www.gao.gov/new.items/d07576t.pdf

No distinction was made in the GAO study between DREs and Optical Scanners.

22. **November 2003- Department of Legislative Services, Maryland General Assembly Commissions the RABA Report found DREs could be hacked in one minute.**

The Report commissioned by the State of Maryland confirmed Diebold's lack of security, the researchers finding the hardware is readily available to an attacker. One team member picked the lock in approximately 10 seconds. Individuals with no experience (in picking locks) were able to pick the lock in approximately 1 minute. [20]

23. All of these independent reports were included along with documented evidence of the voting vendors' illegal and unethical conduct in covering up their failed systems, lying to election officials, misrepresentations, in two memos entitled ***New York State Law Prohibits the State from Entering into Contracts with Any of the Vendors Presently under Consideration,*** July 24, 2007 Memo http://www.votersunite.org/info/VendorsProhibited.pdf and an Updated Memo re: ***Vendors Ineligibility to do Business in New York***, August 22, 2007 http://www.votersunite.org/info/UpdatedVendorIrresponsibility807.pdf, were all submitted to the State Board of Elections, the Office of General Services and the Office of the Comptroller in July and August of this year, but have been ignored by the state officials who have the responsibility for affirmatively investigating the

[20] .RABA TECHNOLOGIES LLC. TRUSTED AGENT REPORT: DIEBOLD ACCUVOTE-TS VOTING SYSTEM (report prepared for Department of Legislative Services, Maryland General Assembly, Annapolis, Md., January 2004) http://www.raba.com/press/TA_Report_AccuVote.pdf

evidence of irresponsible vendor conduct; evidence that would bar the voting vendors from doing business in the state of New York.

24. We have tried to point out to the SBOE, the Governor's office, legislators and county election commissioners that the other states, having wasted millions of tax payers' dollars on these failed systems are either now trying to justify their mistakes by refusing to look at the evidence or have begun lawsuits against the vendors for fraud, misrepresentation, breach of contract, etc.

25. In New York we have no excuse. We have the evidence in front of us and yet our legislators, the Governor's office, the SBOE, all of the entities being represented by the Attorney General 'on behalf of the people' are ignoring the evidence that we have diligently put before them.

26. We respectfully urge the Court to look at this evidence which our state government has failed to consider and to direct a hand count of the two Federal races for 2008 so that regular citizens may have the oversight that is essential if the people are to retain control over the instruments of government we have created.

27. We respectfully ask the Court to permit the *amicus* brief and the declarations from the various *amici* to be accepted so that the Court can view all the evidence and prevent the certain disenfranchisement of New Yorkers were we required to vote using computerized voting systems.

28. In the event the Court directs a hand-count of the two federal races Re-Media will volunteer to assist the county election commissioner in finding citizens to help hand-count our ballots.

I declare under penalty of perjury that the foregoing is true and correct.

_____

/s/ JOANNE LUKACHER

Executed on December 11, 2007