

Voter Verifiable Receipt Accusations

- **TrueMajority.com**
 - States that “They **don't** even have a way to have a **real recount** should the machines crash or there be any other reason to think that something might have gone wrong.
- **Blackbovoting.com**
 - “The newest voting machines **eliminate** the paper trail. Voters and local election officials **no longer** have any way to **verify** that votes are counted **correctly.**”

Media & Web-Site Accusations

- Time Magazine Article
- Vanity Fair Article
- Web-site Review
 - Blackboxvoting.com
 - TrueMajority.com

From Back4Voting Document Archives

Time Magazine – April 26, 2004

“The Vexations of Voting Machines”

- Claims that in three Maryland counties Diebold touch-screens were not displaying the entire ballot.
 - Time magazine claimed that a technician checked the machine and said that the entire ballot was not being displayed.
- This statement is false. The technician testified that he made no such statement. Even the complaining Maryland voter testified that he may have missed the race.
- “..not possible to do a true recount with the system because they produce nothing tangible when a vote is cast.”
- Machines can produce an anonymous printed copy of each ballot which has been used for a recount.
- “..believe that the systems are too vulnerable to tampering or simple breakdowns.”
- Diebold touch screen machines are reviewed by the federal & state testing authorities before they are used in an election. Logic and accuracy tests are also performed by county officials that verify that the machines will work properly during the election and have not been tampered with.

Time Magazine -- April 26, 2004

"The Vexations of Voting Machines"

- *"Possible to vote more than once..."*
- Once the voter casts their vote, the information is erased off of the smart card, making the card useless. The fact is you can't read or write to the card without having the appropriate encryption keys.
- *"...the new machines didn't fire up properly..."*
- This statement infers that the touch screen machines did not work properly. The touch screens performed flawlessly. The machines that this quote refers to are the Precinct Control Modules (PCM) which booted up to an unfamiliar screen due to low battery in isolated locations. Poll workers in most precincts were given the proper instructions to resolve the issue by 7:30am.

FROM THE 2004 TIME MAGAZINE ARCHIVES

Vanity Fair – April 2004

“Hack the Vote”

- Referring to the supervisor smart card, Bev Harris states that, “...every one of these cards had the same password - 1111 hard-coded into the system”
- Diebold has installed a dynamic pin which is controlled by the local election officials. The dynamic pin can have up to 6 digits and can be changed at every election.
- “land line modem...far from hack proof”
- Transmitting election results is optional and the election results are encrypted and digitally authenticated during transmission.

From

Bev Harris Document Archives

Vanity Fair – April 2004

“Hack the Vote”

- *“In a couple of mouse clicks, Harris was able to go in through Microsoft Access, as if through a back door, change vote totals, and erase any ‘audit trail’ of her actions”*
- **There are no back doors. Harris had full administrative rights to the computer she was using, which does not reflect the real-life situation in an election office. Each user has a log-in and password identification, and the server is also physically guarded. Only authorized software can be installed on the server and Microsoft Access is not authorized.**

Web-Site Issues

- No content regulation
- Information posted from unqualified sources
- Information not validated
- Misleading information due to the fact that quotes are used out of context
- There is a small percentage of discussion/debate that is being used to improving the system

From Blackboard Moving Document Archives

Top Activist Web-Sites

- **BlackboxVoting.com**
- **TrueMajority.com**
 - The 2 above web-sites are the major hubs for various other activist sites including:
 - **Wired.com**
 - **VoteFraud.org**
 - **VerifiedVoting.org**
 - **NotablesSoftware.com**

System Security

Accusations

- TrueMajority.com
 - “One hacker (during the RABA testing) was able to open a locked machine and start **changing votes**. It took him less than a minute. Another hacker was able to **intercept and change vote totals** being sent to headquarters.
- Blackboxvoting.com
 - “The machines produce **new tampering and vote-rigging vulnerabilities**. We do not have adequate systems to protect against tampering with programmers, vendors, and technicians.”
- Several activist **web-sites link to the Avi Rubin report stating**,
 - “.a poll worker could **tamper** with the contents of the floppy before inserting ~~it~~ into the voting terminal.”
 - “**Send**ing election results in this way over the **Internet** is a bad idea.”

System Security

Diebold Response

- There have been **ZERO** security related problems reported
- Touch screen **does not** use floppy discs
- Voting terminals are normally pre-loaded, tested and sealed before delivery to precincts
- **Logic and Accuracy tests**, run on each terminal with results verified before and after each election
- The Diebold voting station **does not send results over the Internet**, nor does the voting station connect to the Internet at any time
- Dynamic access **PIN can be changed** by election officials as often as needed
- Many critics disregard real-world processes when examining systems

Smart Card Reproduction Accusations

- Many of the activists' web-sites have made claims including:
 - Smart cards are reproducible and therefore can allow voters to vote more than once.
 - Smart cards provides very little additional security and in fact opens the system to several attacks.

From P. 14 of Voting Document Archives

Smart Card Reproduction

Diebold Response

- Smart cards cannot be reproduced or used multiple times.
 - After serving as an election official during the Maryland primaries, Avi Rubin himself stated, “We made the widely criticized claim that a teenager in a garage could manufacture smartcards and use them to vote 20 times... I now believe that this particular attack is **not a real threat**.. I started realizing that some of the attacks described in our initial paper were actually quite unrealistic.”
 - There have been a variety of real-world voting day checks and balances that many critics have ignored in their laboratory-originated critiques.
 - Once the voter casts their vote, the ballot is erased off of the smart card, making the card useless until re-activated by a poll-worker.

System Issues

Accusations

- **TrueMajority.com**
 - States that election officials are “installing touch screen computerized voting machines that are **vulnerable** to the same problems as other computer technology, including **crashes and power-outages.**”
- **Rebecca Mearns & David Dill Web sites**
 - Both have stated that electronic voting is vulnerable and **unreliable** for modern elections.

System Issues

Diebold Response

- Logic and accuracy tests are run on each terminal by an election official with **results verified** before and after each election.
- **Internal battery** which allows unit to run 8 hours without electricity in case of a power outage
- Units are **independent** of one another, allowing voters to use any of the machines.
- Internal audit logs **record all activities** performed on the systems

From

SAATCHI Archives
Document

Voter Verifiable Receipt

Diebold Response

- The Diebold Election Systems machines have internal printers and **currently** can produce an anonymous printed image of each ballot cast during an election.
 - This allows **verification** during a recount or any other review of the election results
- Verifiable receipts is a matter of public policy, **not** of technological capability.
 - DESI can meet whatever standards are established when this public policy debate is resolved.
- Federal standards **must be established** in order to provide a uniform experience for every voter.
 - Current Federal legislation being considered to mandate VVR.

California Certification Accusations

- [Blackboxvoting.com](https://blackboxvoting.com)

– “... Yet despite warnings from the state's chief elections officer, Diebold continued fielding **poorly tested, faulty software and hardware** in at least two of California's largest urban counties during the Super Tuesday primary...”

From blackboxvoting.com Document Archives