



Statement on Electronic Voting

ACLU of Massachusetts
Science, Technology, and Liberty Committee
May 2004

Introduction

Protecting and promoting the right to vote is perhaps the first democratic imperative. That right is endangered today by the premature use of direct electronic voting machines, or DRE's. While new voting technologies hold great promise, they are not yet sufficiently secure or trustworthy. Until voters can depend on DRE's to record their votes accurately, the American Civil Liberties Union of Massachusetts strongly opposes their widespread use.

A) Voting Technology Requirements

The following requirements must be satisfied by any voting system to be used in Massachusetts.

Accuracy

Every voter has a constitutionally-protected right to cast a ballot that is counted accurately. Adoption of new voting technologies should, at the very least, *not decrease* the accuracy of vote counts in comparison to existing technologies or increase the potential for abuse

Anonymity

Voting systems should allow every voter to cast his or her ballot in secret.

Accessibility

Voting machines should enable all voters to vote irrespective of disability and language ability.

Transparency

Democratic governments are open governments. Just as courts and legislatures are open to the public, so too should the inner

workings of voting machines be open to inspection by the public's chosen expert representatives.

B) The Trouble with DREs

A DRE typically contains a touchscreen that secretly displays a ballot to the voter. The voter touches the screen to indicate his or her intended votes, and the machine records the votes directly in the computer's memory. The votes are counted based directly on these electronic records.

DREs are significantly more susceptible to intentional widespread tampering or unintended bugs than the lever machine or scan-sheet technology currently used in Massachusetts. Through the use of DRE's, election results could be falsified invisibly on a previously-unthinkable geographical scale. A single programmer at a DRE manufacturer could conceivably change the code in many or all of the manufacturer's DREs without detection. Poll workers, hackers, or even voters might also be able to tamper with DREs at individual polling places.. DREs introduce the possibility of statistical tampering – changing the software so that it miscounts an undetect-able, but significant, number of votes in favor of one party and/or candidate.

The inherent difficulty of inspecting and analyzing software makes DRE tampering especially difficult to detect. Moreover, the most recent generation of DRE technology has been supplied to municipalities under restrictive agreements that prohibit public inspection of the DRE's constituent software. In at least one case,

DRE software code became publicly available inadvertently, and computer science researchers who examined the code found significant security flaws in it.

DREs have proven to be problematic in several real elections in states including Florida, New Jersey, and Texas. Current DREs score low on transparency due to the manufacturers' unwillingness to allow expert review of their source code.

C) Recommendations for the 2004 Elections

1. DREs Should Only Be Used for Voters Requiring Them for Accessibility

Existing DREs should not be used as the default voting technology because they are not reliably accurate or transparent and it is not possible to make them accurate or transparent in time for the November 2004 election. DREs should, therefore, only be available where legally and practically necessary to provide access to voters who require them, such as voters with disabilities or language barriers who cannot effectively use non-DRE machines. Other, more time-tested, voting technologies, such as optical scan machines, should be used for all other voters.

2. Any DREs in Use Should be Subject to Strict Certification Requirements

DREs should be required to satisfy strict certification requirements before use. Such requirements must at least include guarantees that DRE source code will be available for inspection by experts chosen by the Secretary of the Commonwealth who have no relationship with the DRE vendor. Certification should also require that at least a sampling of individual DREs be tested on election day to ensure that they are running the same code that was certified.

3. All Voting Machines Should be Subject to Random Testing on Election Day

Procedures should be established for randomly testing individual DREs on election day to ensure their accuracy and significantly increase

the likelihood that bugs or tampering would be detected.

4. Voter-Verified Paper Trails Should be Implemented on DREs as Soon as Possible

When DRE's are essential to providing voter access, they should be equipped to provide voter-verified paper ballots as soon as possible, both to decrease susceptibility to bugs and tampering and enable any desired recounts.