E-Voting in the United States

Donald P. Moynihan
University of Wisconsin-Madison, USA

INTRODUCTION

Many aspects of government have seen improvements in reliability, customer interface, speed, and cost as a result of digital innovations. In some jurisdictions, the most antiquated aspects of government are the voting technologies used during elections. Such technologies are expensive and used infrequently, which discourages public investment in updates. However, in close elections, any unreliability in these technologies can have a major impact on who takes control of government. The 2000 U.S. Presidential election hinged on the state of Florida, where antiquated punch-card voting machines, combined with poorly designed ballots and unclear recounting standards, were blamed for a high degree of uncertainty during a drawn-out recount process.

This chapter looks at the growing adoption of e-voting in the form of direct recording electronic (DRE) machines in the U.S. following the 2000 election. Lawmakers enthusiastically endorsed the concept of e-voting with only a limited understanding of the risks involved. E-voting can be implemented in a number of ways—with or without a printed paper ballot, with open or proprietary software—that affect some of the risks associated with it. But some theorists of complex systems and many computer security specialists warn that any complex technology like e-voting machines are prone to failure and should not be trusted to count votes. A loosely coordinated online protest movement offered the argument that election reformers were moving too fast. E-voting since has received negative press coverage, which, in some cases, has slowed down the adoption of or led to additional requirements on the use of DREs.

BACKGROUND: THE POTENTIAL OF E-VOTING

In the aftermath of Florida, e-voting machines seemed the obvious choice to move election administration into the 21st century. The media pointed to the outdated nature of most election technologies across the country, and many state governments worried that they would be the next Florida. Since elections are administered primarily by state and local governments, there are a variety of election technologies in place, driven largely by the size, resources, history, and preferences of the different counties and townships. These different options include the following:

- **Paper:** Voter marks preference next to printed list of options and drops ballot into sealed box; ballots are counted manually.
- **Levers:** Voter pulls lever next to candidates name; machine records and tallies record.
- **Punch Cards:** Voter uses computer-readable card to mark vote by punching hole into numbered boxes indicated by a ballot booklet or directly onto a ballot card. Computerized tabulation machine reads votes by identifying holes in the ballot.
- **Optical Scanning:** Voter marks computer-readable paper ballot; computerized tabulation machine tallies votes.
- **DREs:** Voters select candidate listed on a computer screen by touching the screen or button directly. Votes are tabulated on a computer.

The last two options are the most reliant on digital technology and the most recent. Up until the 2000 election, about half of jurisdictions used either paper, punch card, or lever. More than 40% used optical scans, and less than 9% used DREs (Caltech/MIT Voting Technology Project, 2001a). Since 2000, DREs have been a popular choice for new systems, and it is estimated that almost one-third of votes in the 2004 elections were counted by a DRE (Seelye, 2004).

The process of voting with a DRE begins when the voter arrives at the polling station and is given a memory card to insert into the machine. Voters select from a touch-sensitive screen or parallel button the candidate of their choice. The votes are tabulated internally by the machine and reported to a central counting station. In the aftermath of Florida, DREs seemed an ideal choice. They claimed to record each vote perfectly and do away with the slow and potentially subjective recounts featuring pregnant, dimpled, or hanging chads. DREs had other advantages: they were user-friendly, reported votes more quickly, prevented voters from voting for more than one candidate in the same race, and reminded voters if they had not voted in a particular election. DREs also offered to help the visually impaired through the use of larger screens and

earphones, prompting support from representatives of the disabled. DREs gave the ability to present the ballot in different languages at little additional expense, which facilitated diverse voting populations.

The effect of Florida brought the usually non-contentious issue of election administration to the top of the policy agenda. The perceived weaknesses of the traditional decentralized election system prompted greater federal-level involvement. In October 2002, the federal government passed the Help America Vote Act (HAVA), which provided federal funding for the replacement of older machines and required that new machines allow for disabled access, which had the effect of promoting e-voting machines.

E-VOTING CONCERNS

Given the advantages of e-voting, it may come as somewhat of a surprise that a number of scholars and commentators, led by computer security specialists, began to raise qualms about its adoption. Three criticisms were made (Moynihan, 2004). The first was that DREs did not count votes as reliably as most alternative technologies. The second was that the reliance on software created the potential for error or tampering. The third was that DREs are currently designed so that such errors are unlikely to be caught or remedied.

A survey by the Massachusetts Institute of Technology and Caltech (2001a) found that in 2000, DREs had higher instances of residual votes (1.6%) than hand-counted paper (1.3%) and optically scanned ballots (1.2%). Residual votes are votes that are lost because voters choose more than one candidate, create an unreadable ballot, or leave a blank ballot. The residual vote is the traditional measure of voting system reliability. It might be expected that as DREs develop better user interface and as voters become more used to them, this rate of error is likely to decline.

The more serious criticisms have to do with the reliance on software, its proprietary nature, and the absence of voter-verified paper votes. Software tends to be complex. Computer security specialist Bruce Schneier (2000) points out, "Even a simple computer program has hundreds of thousands of lines of computer code doing all sorts of different things. A complex computer program has thousands of components, each of which has to work by itself and in interaction with all the other components" (p. 6). More than alternatives, DREs in the U.S. rely on complex software to create user interface and to count the votes. DREs, therefore, can be considered complex systems. Systems theorists, especially Charles Perrow (1999), warn of the tendencies of high-risk complex systems to fail. Perrow's (1999) natural accident theory argues that the central problem of complex systems is that they make accidents inevitable. Errors in multiple parts of complex systems can lead to dramatic and unexpected system failure. The potential for failure increases when the complexity occurs in tightly coupled systems that have the potential for unpredictable feedback loops. System failure, therefore, occurs not as a result of predicted vulnerabilities but as a result of errors occurring and interacting in unexpected ways.

These concerns are echoed by many computer security specialists, who point out that computer systems have bugs that can cause them not to malfunction and stop but, instead, to continue running and behave in ways unintended by designers. In the case of voting, DREs may appear to count votes but may do so incorrectly. There is federal and frequently state testing of DREs machines, but the testing process is opaque. Testing labs are paid by the vendors rather than the government and do not provide information about the nature of the tests or the credentials of the testers (Harris & Allen, 2004). The federal standards against which the machines are tested were revised in 2002 but have been criticized for failing to test commercial, off-the-shelf software used in DREs and because they remain "notably weak in the areas of secure system design and usability" (Mercuri & Neumann, 2003, p. 37). More generally, prevention that relies on verification is always problematic, since testing is imperfect and will miss bugs that inevitably occur in complex software. "Testing for every known weakness is impossible. … Testing for all possible weaknesses means testing for weaknesses that you haven't thought of yet. It means testing for weaknesses that no one has thought of yet; weaknesses that haven't even been invented yet" (Schneier, 2000, p. 337).

In the U.S., election systems are provided by private-sector vendors. The oligopoly of three firms that dominate the market for DREs has reduced further the transparency of the software. Vendors use proprietary software, which means that, apart from outside testers, no members of the public can view the underlying computer code. The vendors argue that they have a commercial interest in maintaining the secrecy of their product and that such secrecy reduces the potential for hackers to introduce bugs into the system. This security-through-obscurity approach has been criticized by security specialists as being outdated; it lost credibility when a copy of the source code of one of the primary vendors, Diebold, became available on the Internet. Computer security specialists at Johns Hopkins University and Rice University undertook a line-by-line analysis of the source code, which revealed several vulnerabilities within the software and led them to conclude, "The model where individual