The John Marshall Journal of Information Technology & Privacy Law

Volume 23
Issue 3 *Journal of Computer & Information Law - Spring 2005*

Article 1

Spring 2005

Foreword, 23 J. Marshall J. Computer & Info. L. 485 (2005)

Leslie Ann Reis

ARTICLES

FOREWORD

LESLIE ANN REIS†

"It's not the voting that's democracy, it's the counting."[1]

And, it's the counting, more precisely, the technology used to cast and count votes that has become the focus of noisy national debate. In 2000, much of the controversy surrounding the presidential election, including the contentious and chaotic ballot recall in Florida, centered on the use of punch card voting technology – a technology that had been in use since the 1960's.

In an effort to prevent the same problems that sent the 2000 presidential election to the Supreme Court, technological and legislative solutions were suggested. Congress passed the Help America Vote Act ("HAVA") in October 2002.[2] HAVA was intended to improve the administration of state and federal elections through three primary vehicles. First, HAVA "establish[ed] a program to provide funds to States to replace punch card voting systems."[3] Second, it created a new federal agency "to assist in the administration of Federal elections and to otherwise provide assistance with the administration of certain Federal election laws and programs."[4] Finally, HAVA mandated that "minimum election administration standards"[5] be developed for states and local governments having responsibility for administering federal elections.

Since the 2000 presidential election debacle, prompted in part by HAVA, we have seen the development of voting technologies that provide the promise of solutions – the end to hanging chads and misplaced paper

† Director and Adj. Professor of Law, Center for Information Technology and Privacy Law, The John Marshall Law School; Faculty Editor, *The John Marshall Journal of Computer and Information Law.*

1. Quote Details, *Tom Stoppard: Jumpers Act 1 (1972)*, http://www.quotationspage.com/quote/ 23659.html (accessed Dec. 2, 2005).

2. Pub. L. No. 107-252, 116 Stat. 1666 (2002).

3. *Id.* at preamble.

4. *Id.*

5. *Id.*

ballots, along with the assurance of verified voting and easy methods of recount. Moreover, as the 2006 deadline for meeting HAVA's requirements for replacing outdated voting systems approaches, we have also seen a rush by states, counties and local governments to implement these technologies.[6] There are two common types of electronic voting systems: optical scan systems that use an electronic reader to record votes and direct recording electronic systems ("DRE") that include the hardware and software used to generate ballots, cast and count votes, and sometimes maintain audit information.[7] Simply, DRE systems allow voters to cast their choices directly on an electronic ballot rather than on a paper one.

There are many advantages to electronic voting systems. Efficiency and accuracy are perhaps the most obvious. By automating the election process, human error that may be injected into the process by voters and election workers, is reduced. Moreover, electronic voting systems are adaptable and can be programmed to allow for ballots in multiple languages or accommodations for voters with disabilities.[8]

But, electronic voting is not a panacea. Critics claim that the technologies employed have inherent security problems, that there are flaws in system security, access and physical hardware controls that could permit the machines to be hacked, thus opening the possibility of widespread electoral fraud.[9] In addition, transparency and accountability issues exist with the actual working of the machines. Voting machine software is proprietary and manufacturers have fought, albeit unsuccessfully, to keep their computer codes secret.[10] Moreover, some opponents claim that because a number of systems do not require paper-back-up records or other means of verification, there is no way to assess the accuracy or integrity of the electronic voting machines or election results.[11]

In the 2004 presidential election, more than 40 million voters cast their votes on approximately 175,000 recently installed electronic voting

6. Mark L. Songini, *E-voting Grows Without Consensus*, Computerworld (Oct. 31, 2005) http://www.computerworld.com/securitytopics/security/story/0,10801,105802,00.html (accessed Dec. 2, 2005).

7. Government Accountability Office, *Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Underway, But Key Activities Need to be Completed*, at 7 GAO-05-956 (Sept. 2005) [hereinafter *"GAO Report"*].

8. *Id.*

9. *Id.* at 22.

10. *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (D. Cal. 2004).

11. *See generally* Verified Voting Foundation, *VerifiedVoting.org Index*, http://www.verifiedvoting.org (accessed Dec. 2, 2005); Black Box Voting, *A Diebold Investor Asks a Question*, http://www.blackboxvoting.com (accessed Dec. 2, 2005).

machines.[12] While most of the machines functioned correctly, a number of problems were reported. Some of the most serious problems involved flaws in equipment design and security programming, including the lack of encryption for cast ballots and audit logs allowing for possible undetected alteration and faulty security protection for ballot files that determine how the ballot will look and work. These faults potentially allow a vote cast for one candidate to be recorded as a vote cast for another.[13]

In one county in Florida, electronic voting machines failed to activate correctly, causing extensive delays in the opening of polling places. In another instance in the same county, electronic voting machines malfunctioned and recorded approximately 3,900 votes too many for one of the presidential candidates.[14]

A county in Pennsylvania made a ballot error on an electronic voting system that resulted in many votes not being correctly counted. The county's undervote percentage reached 80% in some precincts.[15]

Electronic voting machines in North Carolina lost more than 4,000 votes when they continued to accept votes after the machines' memories were full.[16]

In spite of the reported glitches with electronic voting technology, the use of such technology during the 2004 election was largely successful. As a consequence, manufacturers of electronic voting machines have declared victory for the technology.[17] However, even though the problems that emerged during the 2004 presidential election did not affect the outcome of that election, trouble continues to plague state elections this year.

A city in Ohio contested the results of the recent election, claiming that the results of a fire levy referendum was invalid because it could not be determined whether voters received the correct ballot on the newly installed electronic voting machines.[18]

Plans to use newly acquired electronic voting machines for the November 2005 municipal elections in a New Mexico city were scrapped when it was discovered that the software programmed into the machines

12. Caron Carlson, *E-voting Returns Mixed Results; Disruptions Point to Unresolved Problems*, eWeek 1 (Nov. 8, 2004).

13. *GAO Report*, *supra* n. 7, at 2.

14. *Id.* at 31.

15. *Id.* at 29-30.

16. *Id.* at 31.

17. *See* Dan Verton and Patrick Thibodeau, *Electronic Voting Systems Pass Their Big Test - Maybe*, Computerworld 1 (Nov. 8, 2004); Caron Carlson, *E-voting Returns Mixed Results; Disruptions Point to Unresolved Problems*, eWeek 1 (Nov. 8, 2004).

18. Bob Fitrakis and Harvey Wasserman, *Ohio's Diebold Debacle: New Machines Call Election Results into Question*, The Free Press (Nov. 24, 2005) http://www.freepress.org/departments/display/ 19/2005/1593 (accessed Dec. 2, 2005).

contained incorrect information.[19]

In two Ohio counties, electronic vote totals were so delayed that results could not be posted until the morning after the election.[20]

Technical problems with electronic voting machines that may have affected the outcome of local elections were reported by voters in Virginia and Pennsylvania.[21]

In October 2005, the Government Accountability Office ("GAO") released a comprehensive report analyzing the issues raised by the increasing use of electronic voting systems.[22] The report states that "significant concerns about the security and reliability of electronic voting systems"[23] have been raised and that "some of these concerns have been realized and have caused problems with recent elections, resulting in the loss and miscount of votes."[24] Further, the GAO identified a number of specific problems with security and reliability of electronic voting systems. These problems include: weak system security controls, design flaws in audit trail systems, incorrect system configuration, vague and incomplete security provisions, inadequate security testing, lack of transparency in the testing process, inadequate requirements for vendor documentation, poor implementation of security procedures, weak security management practices and system failures during elections.[25]

The GAO found that there is still much work to be done to improve electronic voting systems and continued government efforts are necessary. The GAO noted that "there is a lack of consensus among election officials, computer security experts, and others on the pervasiveness of these concerns."[26] But, it concluded that the problems and concerns "merit the focused attention of federal, state and local authorities responsible for election administration."[27]

In addition to the concerns raised by the GAO report, we continue to see problems, controversies and legal challenges involving many aspects of electronic voting technologies. As this issue of the *John Marshall Journal of Computer and Information Law* goes to press, controversies involving security provisions, verification systems and state certification

19. Steve Ramirez, *Glitch Found in New Voting Machines*, Las Cruces Sun-News 1 (Oct. 29, 2005).

20. Peter Bronson, *How Your Ballot Dodged Many a Bullet Amid Election Night Chaos*, The Cincinnati Enquirer, 13C (Nov. 17, 2005).

21. *See* Cody Lowe, *Election Questions Turn Touchy*, The Roanoke Times A1 (Nov. 29, 2005); Tom Coombe, *Recount Ordered in Upper Mount Bethel*, Morning Call B9 (Dec. 3, 2005).

22. *GAO Report*, *supra* n. 7.

23. *Id.* at 22.

24. *Id.* at 23.

25. *Id.* at 24.

26. *Id.* at 23.

27. *Id.*

of electronic voting machines are making headlines.[28] Of note is the highly contentious legal battle involving the certification of electronic voting machines in North Carolina – a case the *Journal* will be following in future issues.[29]

It is clear that there are many interests at stake; politicians, federal, state and local governments, the commercial technology industry and of course the voting public all have a stake in the outcome of the issues arising from the increasing use of electronic voting technologies. The challenge remains to find a balance between election integrity, accountability, transparency, voter privacy and the intellectual property rights of inventors and manufacturers of electronic voting equipment. Obviously, electronic voting is, and will continue to be, a hot topic.

To help practitioners, election officials and the public understand the underlying legal, technical and policy issues surrounding the use of electronic voting in the 2004 general election and beyond, the Center for Information Technology and Privacy Law at The John Marshall Law School conducted a day-long symposium entitled "E-lection 2004: Is e-voting ready for prime time?" The symposium brought together many of the top technical, legal and academic minds who were at the forefront of the new voting technology to discuss, debate and speculate on the future of electronic voting in the United States.

The *Journal* recognizes that this topic is of major importance and will continue to influence information law and policy in the United States for years to come. We believe that government, academia and the information technology and computer security industries must work together to design a framework for resolving these issues while balancing the interests of all concerned. Thus, we proudly present in this issue presentations and papers from several of the symposium participants, including an overview of the importance of the voting process as a means to transfer power that was presented by Richard C. Balough, the Associate Director of the Center for Information Technology and Privacy Law; a hands-on description of what occurred in Florida after the 2000 Presidential election and how Florida changed its laws to prevent a recurrence, by Lida Rodriguez-Taseff, Counsel and Chair of the Miami-Dade Election Reform Coalition; an analysis of what went wrong with electronic voting in two 2004 North Carolina state races written by Lillie Coney, a senior policy analyst for the Electronic Privacy Information

28. *See e.g. Voting Machines and Instant Runoffs*, N.Y. Times 14LI 23 (Dec. 4, 2005) (discussing certification and verification); *On Voting Machines*, The Sacramento Bee (Dec. 1, 2005) (addressing security and certification issues); William Presecky, *Kane Launches Electronic, Early Voting Initiatives*, Chicago Tribune W4 (Nov. 30, 2005) (examining impementation and certification concerns).

29. *Diebold Election Systems, Inc. v. The North Carolina Board of Elections, et al.*, 05 CVS 15474 (Super. Ct. Div., N.C. 2005).

Center; an examination of the intersection between copyright, security and free speech in the recently decided *Online Policy Group v. Diebold*[30] case by Doris Estelle Long, Chair of the John Marshall Law School's Intellectual Property and Information Technology and Privacy Group; and a wrap-up of the 2004 election and why it exceeded the margin of litigation written by Doug Chapin, the head of electiononline.org, a non-partisan organization dedicated to providing up to date information on electronic voting.

Also included in this issue are the winning briefs and bench memorandum from the 23rd annual John Marshall International Moot Court Competition in Information Technology and Privacy Law. Each year, the competition attracts teams from all over the world who brief and argue cutting-edge legal issues in information technology and privacy law that are interwoven in a contemporary factual setting. This year, the problem involved technologies affecting the privacy rights of a political candidate. The problem and bench memorandum were created by a group of John Marshall students, led by Patricia Gerdes. Ms. Gerdes unexpectedly passed away in early 2005. The *Journal* joins the entire JMLS family in mourning her untimely passing. Ms. Gerdes was a *Journal* candidate, an exceptional student and research assistant. Her passion, energy and contributions to the *Journal* and the law school as a whole will not be forgotten. She is deeply missed.

We dedicate this issue of the *John Marshall Journal of Computer and Information Law* to the memory of Patricia Gerdes.

30. *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (D. Cal. 2004).