Managing Technological Change in Elections

Tim W McGraw[1]* and Craig Fisher[2]

ABSTRACT

While there is no way to guarantee the security and integrity of internet or electronically base voting systems, more research can be conducted toward a means to creating such an environment. Through the implementation of communities of practice as learning organizations, involvement in the design and testing of i- and e-voting systems can be inclusive of all constituencies and can produce a more robust design standard than proprietary solutions can achieve.

Keywords: e-voting, i-voting, communities of practice, elections, learning organizations, SERVE

1. Introduction

Direct recording electronic systems, or DREs, have been put forth as one solution to problems such as were experienced in Florida in the 2000 presidential election, and internet based voting has had success in highly controlled, limited testing. Variations of both electronic and internet voting are increasing in use. Corporate proprietary voting systems pose problems in standards and transparency of testing. Constraints to process control and software validation raise questions with respect to malfeasance as well as programming and procedural error. The internet is subject to attack from anywhere in the world, and neither prevention nor detection of attacks can be assured. Even if the machines employed to conduct elections, whether kiosks or our own home computers, were able to be secured beyond doubt, procedures for elections administration would still need to be addressed. From paper ballots to lever machines, punch cards, mark-sense ballots and ultimately DRE and internet based voting, new technologies bring new methods and each change brings uncertainty and adds complexity.

To date, little research has been conducted toward identifying organizational approaches to managing what appears to be an unstoppable migration toward the use of technology in elections. Each technology over time has exhibited flaws, yet the integration of new systems brings instabilities with far greater potential for catastrophic results, because failures in older elections technology affected only a localized area. Mass introduction of internet or DREs can have unforeseeable and uncontrollable effects on the outcomes of elections.

2. Obstacles

A July, 1999, ABC News national telephone poll showed that the majority of 18-49 year old voters support virtual voting, while Americans age 50+ do not[2.] Some believe that the race to embrace DRE and internet voting is borne of naïve trust in technology, and that the potential for unanticipated consequences is being

[1] Marist MSTM Program, Poughkeepsie, NY, USA
* *Corresponding Author:* (Email: timothy.mcgraw1@elearning.marist.edu Telephone: +845-437-7292)
[2] 3399 North Rd, Poughkeepsie, NY 12601, USA

overlooked. Members of the ACM and others have published work that suggests that there is a long way to go before technology can be secure in elections.

Meanwhile, elections officials find themselves in a position of having to use DRE and other methods of computerized voting, without knowing how the systems work, how to detect problems, or how to recover from failures. Costs of these systems also suggest that once municipalities have committed to a choice in technology, they are not likely to reverse their decision. In such cases, inadequately designed systems may be making their way into service around the US with little or no oversight. Electronic and internet voting systems suffer from mutually exclusive requirements that prevent the automation of audit verification; the need for privacy and auditability together. "The lack of standards, legislative loop-holes, trade secrecy, usability problems, privacy, security, and other inherent computer issues results in a dangerous “Trust-us” mentality. Transparency in the process is essential, not only to provide auditability, but also to enhance voter confidence."[5]

Voter Verified Physical Ballots as described by the Mercuri Method require that voting machines incorporate a printed paper ballot that is displayed behind a glass partition to the voter. If the paper printout does not match the voter's intentions, they can call upon an election official to void their vote and allow them to recast their ballot. One possible issue with this system is that while paper ballots are available for recount, there is no guarantee that the vote that is stored electronically matches the vote displayed to the voter. In cases where voting machines change only one vote, such discrepancies would still be virtually undetectable. Some vendors have claimed that the need for voter-verifiability can be met by printing a batch of paper ballots after the elections close, however this provides no assurance that the printed vote matches the intentions of the voter, nor a way to verify this. Receipts for votes cast would allow the voter to take home the vote as they cast it, however they provide no real way of administering a recount as it would be problematic to recall all the receipts necessary in a given race, and they make voters susceptible to vote buying and selling as well as other forms of coercion.

3. Direct Recording Electronic Systems

Direct recording electronic systems were intended to end Florida’s nightmare from all manner of punch card difficulties. Additionally, voter error control and correction were thought to address the confusing print layouts of some ballots. Better overall user friendliness and speed of reporting are also touted as benefits of e-voting systems. While these attributes do exist, there are problems with unanticipated DRE behavior, whether in uncounted or misattributed votes, or crashes. Programming bugs can result in systems crashes, which are relatively easy to detect and normally recoverable with a restart, yet more subtle errors can result in undetectable changes that can affect the outcomes of an election with as few as one vote changed per machine.[4]

The risks in e-voting systems arise in nearly every respect, including design, software engineering processes, protective measures, and testing. The Hursti attack and the Princeton group’s Diebold virus are two well known failures of e-voting systems development.[3] Flaws in E-voting testing methods as detailed by Songini, the VoteHere, Inc. system break-in reported in the NYTimes, and numerous problems related to machines in service have been published about elections around the country. Jefferson et. al. assert that various deficiencies and security vulnerabilities exist, that software is closed and proprietary, that qualification and certification do not have adequate oversight and scrutiny, that they are vulnerable to insider programmer attacks, that there exist no voter-verifiable audit trails, and denial of service attacks. In December 2006, Maryland Senate president Michael Miller changed his stance on support of a bill that would require e-voting to include a paper trail. In January 2007, the NYS Board of Elections suspended testing of electronic voting machines because of flaws in the test methods of the company it had hired to perform the tests. Xenakis and Macintosh also note that efficiencies are not gained when traditional counting of paper ballots must complement the use of DREs, raising the issue of cost as a main proponent of rapid deployment of such systems.

4. Internet Voting - SERVE

One major experiment in internet voting has been SERVE: The Secure Electronic Registration and Voting Experiment. SERVE is an internet voting system developed by Accenture and its subcontractors for the U.S. Department of Defense FVAP. The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) allows U.S. citizens who are members of the military services, their family members, and nonresident U.S. citizens to both register to vote and cast their ballot via the Internet, from anywhere in the world. "It is meant to be a complete, Independent Testing Authority-qualified and state-certified voting system that collects real votes."[7] SERVE uses JavaScript, along with either Java or ActiveX scripting, and session cookies in a web browser, and thus will work on nearly any computer. Security is provided within the browser application, by the Secure Socket Layer (SSL) protocol. Once an SSL connection is established, an ActiveX control is downloaded and run.[7]

Since the system uses the voter's own machine as the platform to conduct the transaction, all of the security issues relating to internet enabled computers are relevant, including denial-of-service attacks, spoofing, and viruses. While criticisms of DRE systems have included that software is closed and proprietary, certification standards are lax or non-existent, that DREs are susceptible to programmer error and deliberate tampering, and that no voter-verified audit trails exist, the same criticisms and vulnerabilities apply to SERVE. Further, Jefferson asserts that these vulnerabilities cannot be eradicated in the foreseeable future based on existing architecture.

Jefferson warns that detection is as essential as prevention, and that the subtlety of certain attacks or errors can make them effectively undetectable. An example of one possible transgression available to elections officials includes monitoring individual votes in real time, destroying the essential attribute of privacy. Since personal computers are often not well protected from internet attacks, voters' machines would be especially vulnerable to manipulation. Modified programming that alters votes cast or prevents certain voters from casting a ballot could be employed, either through modification of the election programming source code itself or by the introduction of viruses or Trojan horses, and these cannot be blocked with absolute certainty since anti-virus programs can check only for known viruses.

Man-in-the-middle attacks can be employed to insert the attacker between the voter and the election authority, by forwarding information back and forth to each party. Voters could also be convinced through a carefully designed website that what they were seeing is the authentic voting website, when in fact they could be unknowingly redirected to a different server. Denial of service attacks are also prevalent and there is no way for the SERVE system to circumvent these with certainty.

5. Arizona Democratic Party

In Arizona in March, 2000, the Democratic Party allowed internet voting for the election of its delegates to the Democratic National Convention. Though a private election, registered Democratic voters could vote online for four days. Voters received PINs generated by Election.com, the company administering the election, and had to answer two personal questions before casting their ballot online. Turnout was mixed; high in normally low turnout areas, and low in normally high turnout areas. The timing of the election however suggested that many eligible voters may not have participated, calling into question the claimed successes of the trial.

6. Access

Certain aspects of internet and DRE voting may assist voters with disabilities relative to technologies currently in use. Visual, auditory, other physical disabilities and those with multiple disabilities can all be assisted in various ways if systems are developed to address them. Currently, systems are designed with little thought toward accessibility, and policy to incorporate such design will be necessary. Other issues of access relate to the digital divide and speak to issues of class and race as well as ability.

Internet voting implicitly requires that, in trade for the added convenience of voting at home at any time, the voter must have a computer and internet connection. Costs of such equipment and services vary and are not affordable by all citizens in all areas, raising the question of internet voting as a disadvantage to the poor. Similar problems arise in discussions of online voter registration. While internet use continues to become more widespread, there is the potential in the future for online voting to deliver on its promise of increased voter participation, however several groups were confirmed in the 2000 Arizona Democratic Primary to have been less likely to use available internet voting, including women, the elderly, the non-white, the unemployed, and rural residents. "Internet voting seems likely to weaken the voting rights of minorities, as in this particular case minority turnout dropped substantially more than did white turnout. As long as the digital divide exists in American society, those behind the digital divide will not see enhanced political representation as a result of Internet voting"[14.] The societal implication of the adoption of internet voting is that since certain demographics have greater access to or comfort with the internet, shifts in representation would result from shifts in those voting by a certain method.

7. Management difficulties

Singapore: While some examples of successful e-government exist, they are a microcosm of the issues relating to electronic and internet voting in the United States. Singapore was able to conduct a pervasive and well coordinated transition to e-government services, however its culture and governmental organization were better suited to the transformation than are those of the US. Singapore is a flat, centrally controlled government, able to enforce mandates and provide resources. E-government also represents a more unidirectional flow of information that is also less sensitive than voting information. Ke and Wei warn that lessons from Singapore's implementation do not necessarily hold for cultures of individualism and that success in Singapore cannot be directly correlated to e-government in general.[9]

Complicating the development and implementation of consistent elections technology policy in the US is the decentralized structure of elections oversight, maintained by states and local agencies. While much research has been done on computer security, there is less known about human operational failures within the election process. Technological development must take this into account, and election systems must address overall the organizational issues that can lead to failure. This poses significant problems because DRE and internet voting systems are too complex to be understood and monitored effectively by elections officials. Such expertise is not likely to be available to most precincts.[12] For this reason and due to the closed proprietary nature of many systems, vendors must be relied upon to conduct elections smoothly. This introduces opportunities for error and tampering that cannot be ignored without a cost to public trust and confidence, and which must be addressed by comprehensive policies, created and enforced by groups of knowledgeable and dedicated participants throughout all phases of elections administration.

8. Threat model

Barr suggests a threat model to inform systems testing and certification; wherein a detailed set of criteria exist against which to test any voting system. Without such a model, neither the integrity nor the accuracy of the voting process is assured.[3] Current standards are nebulously defined, and "fail to make precise the usability requirements outlined by HAVA. They confuse requirements for accurate voting with requirements for simplifying system testing. They include seemingly arbitrary specifications; for example, the acceptable error rates (Vol. I, Sec. 3.2.1) seem to have been chosen arbitrarily. They mandate impossible features; for example, they require that shared resources not leak information (Vol. I, Sec. 7.5.4), even though there is no way to prevent this leakage."[3] Since no standards exist for such tests, but the requirement exists for systems to pass, programmers have devised dangerous workarounds such as displaying a message on startup that simply reads, "System Test Passed," though no real test was performed. Vendors pay independent testing authorities, causing conflicts of interest in certifying systems. "These standards, promulgated first by the Federal Election Commission, then by the Election Assistance

Commission (EAC), do not express a coherent set of requirements for electronic voting systems. They contain no system model or threat model."[3] To be effective, such models must address both the programming code that governs the behavior of DRE or internet voting programs, as well as procedural and organizational considerations. "Verification at the receiving station is necessary but insufficient. A man-in-the-middle attack takes advantage of just this type of scenario, where verification is not performed by both parties."[3] By using systems and threat models, there exists a framework within which the specific requirements and criteria for success of a voting process can be evaluated, and evaluations could be submitted from diverse sources including the academic and computer science community, sociologists, and interested citizens, for example.

AccuPoll and Avante both produce DREs with paper records for voters, and Avante's system can be used to print optical scan ballots for vision impaired voters. Optical scan systems by design provide a verifiable paper trail. Hybrid systems incorporate aspects of both paperless DREs and optical scan systems. Chaum suggests a system using elaborate print cryptography. Open source code with voter verifiable paper ballots is being developed by software engineers and computer scientists at openvotingconsortium.org. While there seems to be consensus on the need for voter verifiable paper trails, few provide answers on the range of potential for malicious or error prone programming code. Consensus in this regard focuses on the need to minimize the risks to any system, as well as to assert that these risks and others, such as DoS attacks during elections, can never be fully eradicated. There is disagreement as to the time necessary to resolve issues surrounding DRE voting, though experimental testing and incremental introduction of the technology is recommended. The Internet Policy Institute distinguishes between poll site voting and the use of kiosks as one opportunity for incremental research. They and others also recommend an approach to research incorporating experimentation, modeling and simulation. While each of these efforts represents isolated progress in specific arenas relevant to internet voting, an overarching strategy must at some point emerge to unify the architecture and elucidate gaps in research. Avizienis, et. al. assert that the fault-error-failure model is central to the understanding and mastering of the various threats that may affect a system, and enables a unified presentation of these threats, while preserving their specificities.[6]

9. Systems Theory

Natural accident theory shows that complexity and failure of systems is directly related[1] Errors can cause unintended consequences and may be attributable not to one specific contributing factor or cause, but to interactions among several features within a system. High-reliability theory prescribes ways to address such problems in a systems development and change management context. Hardware, software and human interaction are all essential aspects of defining robust elections. Proprietary approaches to software development lend the opportunity for backdoors and easter eggs through which elections can be manipulated, making clear that external oversight is necessary to ensure properly developed systems.

High reliability theory incorporates the notion that variability is key to minimizing the frequency and effects of accidents within complex systems. "The specialization of different actors in the process reduces the awareness of interdependencies and creates limited understanding of important processes. The operating scale of the system grows rapidly with little time to build a bank of experience, and the infrequency of elections provides limited opportunity to build experience in dealing with problems."[1] Training is therefore an essential part of voting systems design; as important as transparency and auditability.

Open source software has been put forth as a viable approach to developing trustworthy election programs. Inherently, open source allows a greater number of interested parties to participate in development and evaluation. Competing interests with equal access to systems in development can provide checks and balances and ensure a level playing field. Public oversight would be possible, and strengthen systems

against attack. Vendors have lobbied strongly against this, yet proprietary control might still be afforded them for such aspects as user interface and election official training and support.[1] Flaws in elections systems cannot be identified solely by elections officials, who often do not understand the technology and who do not administer elections frequently enough to learn from subtle or undetectable mistakes. Open source development would allow a much wider base of interested parties to contribute, and here is an area where the internet can be employed to greatest effect. Moynihan warns that individual discretion will remain a necessary element in recovering from unforeseen, isolated incidents; however this does not undermine the value of a global approach. Further, there must exist a procedural structure to ensure that any agreed upon software, whether open sourced or proprietary, is verifiably the version that is installed and in use in each DRE machine on election day, and that software used post-ballot casting, for example to transfer results from precincts, is also traceable.

10. Officials and Voters Need to Learn

Voter-verified paper copies of DRE votes provide redundancy. External review provides for unbiased oversight. "Perrow (1999) argues for increasing the oversight of interested parties in the systems environment, while Frederickson and LaPorte (2002) point to the need to examine operational information and to create incentives to find and eliminate error."[1]

The organizational structure of elections in the US is unable to cope with the scope and speed of changing technology, yet it can offer no resistance to the pressure to adopt new technology regardless of its strengths or weaknesses. Adaptation of existing election boards, and officials in short-lived or limited terms of office, are ill-suited to lead the transformation to stable electronic voting. They need training and support from the academic, civic and computing communities. Furthermore, the training and support necessary to protect and secure elections must be ongoing. Threats and vulnerabilities to elections will evolve over time, and the policies and implementations to respond to them must develop as dynamically. To this end, communities of practice in place throughout the elections system, involved directly in elections administration and incorporating disparate points of view and diverse expertise, should be created as learning organizations to maintain oversight, communicate knowledge, and facilitate adequate monitoring over all voting systems regardless of the level of technology employed in each instance.

11. Communities of Practice

Wenger's concept of Communities of Practice represents groups of people with a shared set of stable cultural practices that help define membership in the group.[15] CoPs provide a structure within which groups can participate and collaborate in a process of organizational learning. One example of an online CoP that might serve as a model for a group addressing elections is Company Command (www.companycommand.com), an online community of some 10,000 members of the US Army located worldwide.[15] While these members are geographically dispersed and would not have the opportunity without the existence of the internet to collaborate and share information, Company Command affords them the opportunity, through the C4P model of communities of practice to share and search information. The framework includes content, conversation, connections, and context, to create an environment incorporating multiple perspectives on a given topic or problem. "There is an ebb and flow between tacit and explicit as the knowledge is constructed by individuals, shared, and reconstructed by someone else."[15]

This approach is readily applicable to elections systems development that encompasses more than just the casting of ballots and addresses organizational and procedural questions relating to such aspects as voter registration, aggregate vote tabulation (above the precinct level) and disputations and recounts. Particularly relevant to the problem of decentralized control over elections by state and local governments is that Communities of Practice are not only scalable, but benefit from network externality, in which the value of information increases exponentially with membership, and this is might directly benefit the creation of a nationwide elections structure, without relying on a federal agency for its design or maintenance.

Designed with intent to facilitate a learning organization, CoPs can create, acquire and transfer knowledge about the challenges facing election change, and in turn challenge established principals effectively.[16] In addition to identifying problems such as proprietary closure of software code, CoPs can identify solutions through wide membership and an online platform to archive and develop knowledge among group members. Open source software development specifically is an example of a particular type of CoP; the Network Army. With thousands of software developers who are passionate about their craft, leadership is provided by moral and intellectual influencers and membership is diverse and balanced.[17]

A CoP can provide an organizational learning support system with cognitive maps of information relating to elections issues. Cognitive maps can assist in presenting problems, drawing critiques and suggestions, and fostering the creation of new knowledge. "A Collective Cognitive Mapping System, has four main components: a local (or episodic) memory as the container of individual cognitive maps; a global (or organizational) memory as the container of collective cognitive maps; a local cognitive map generator converting individual beliefs into graphical maps; and a central cognitive map generator collecting cognitive maps of all members and providing a collective view of business problems."[16] A cognitive decision support system uses collections of case studies, cognitive maps and scenarios to create an environment to easily capture searched information and identify tacit assumptions, according to Chen, et.al., allowing them to be integrated into a cohesive bundle with various types of collaborative software and media.

"We recommend as a guiding principle the transformation of individual knowledge into organizational knowledge, a dynamic process involving six knowledge management tasks: knowledge identification, acquisition, validation, maintenance, dissemination, and interpretation. Organizations might have to perform them iteratively to foster shared knowledge and understanding."[16] This type of approach when combined with open sourcing and threat and systems modeling can provide an effective means of assuring that knowledge about elections systems that may be subject to hoarding by proprietary vendors, or undiscovered as a result of ignorance, will be uncovered, shared, and acted upon as quickly as possible. In the context in which deployments of unsecured and untested voting systems has already begun, this approach provides an efficient means of maintaining control over future elections developments.

12. Concluding Remarks

"To protect the accuracy and impartiality of the electoral process, ACM recommends that all voting systems—particularly computer-based electronic voting systems—embody careful engineering, strong safe-guards, and rigorous testing in both their design and operation. In addition, voting systems should enable each voter to inspect a physical (for example, paper) record to verify that his or her vote has been accurately cast and to serve as an independent check on the result produced and stored by the system. Making those records permanent (that is, not based solely in computer memory) provides a means by which an accurate recount may be conducted. Ensuring the reliability, security, and verifiability of public elections is fundamental to a stable democracy. Convenience and speed of vote counting are no substitute for accuracy of results and trust in the process by the electorate."[21] Both hardware and software problems continue to plague not only the prospect of internet and electronic voting, but of the wider use of the internet itself. Elections are of fundamental importance to the functioning of democracy, and to ignore vulnerabilities in such systems is to invite serious consequences for society. Hardware and software issues are not exclusive challengers to elections integrity, however. Elections officials are at a deficit in understanding technology, and are unable to cope with the changes introduced by the new technology in ways that retain the integrity of the elections process. Government officials are likely to respond unpredictably at the specter of potential shifts in voter behavior, and as such are unlikely candidates as leaders of initiatives to preserve and protect voter's rights. Meaningful standards for electronic and internet voting have not been articulated, nor are there organizational structures within government to develop, maintain or enforce them. Many have suggested specific ways to address isolated problems, such as voter

verifiability and proprietary software code, however a more inclusive approach to election systems development is indicated. Large numbers in membership with diverse backgrounds, ideologies and expertise will serve to strengthen the body of knowledge about how we vote, why we vote, and how we can vote in such a way that our vote is counted. An open community of practice that incorporates not only software development, such as openvotingconsortium.org, but also representatives from government and citizens from throughout the world, could contribute not only to the development of the strongest voting systems possible, but importantly to the administration of elections and the protection of democracy in the future. The use of systems theory, threat modeling and open source software development can provide a viable architecture for such a group to flourish.

References

1. Moynihan, D. P., "Building Secure Elections: E-Voting, Security, and Systems Theory," Public Administration Review, September/October 2004, Vol. 64, No. 5
2. ABC News.com Poll: Virtual Voting, July 18, 1999, http://abcnews.go.com/images/pdf/796a2VirtualVoting.pdf
3. Barr, E., Bishop, M. & Gondree, M., "Fixing Federal e-Voting Standards," Communications of the ACM, March 2007/Vol. 50, No. 3.
4. DiFranco, A., Petro, A., Shear, E. & Vladimirov, V., "Small Vote Manipulations Can Swing Elections," Communications of the ACM, October 2004, Vol. 47 No. 10.
5. Mercuri, R., "A Better Ballot Box," IEEE Spectrum, October 2002
6. Avizienis, A., Laprie, J., Randell, B. & Landwehr, C., "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, January-March 2004, pp. 11-33
7. Jefferson, D., Rubins, A.D., Simon, B. & Wagner, D, "Analyzing Internet Voting Security," Communications of the ACM, October 2004, Vol. 47 No. 10, pp. 59-64
8. Wang, C. & Leung, H., "A Secure and Private Clarke Tax Voting Protocol without Trusted Authorities," ACM International Conference Proceeding Series, Vol. 60, Proceedings of the 6th International Conference on Electronic Commerce, pp. 556-565
9. Ke, W. & Wei, K. K., "Successful E-Government in Singapore," Communications of the ACM, June 2004, Vol. 47 No. 6.
10. "Electronic Voting Security Firm Hacked," The Associated Press, December 29, 2003
11. Juels, A., Catalano, D. & Jakobsson, M., "Coercion Resistant Electronic Elections," ACM WPES '05, November 7, 2005
12. Saltman, R. G., "Computers and Elections," ACM '75 Panel on Computers and Elections, pp. 3-7
13. Songini, M. L., "New York Halts E-voting Machine Testing," Computerworld, January 29, 2007, Vol. 41, Issue 5, p. 8
14. Alvarez, R. M. & Nagler, J. "The Likely Consequences of Internet Voting for Political Representation," Alvarez and Nagler, Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1115-1152
15. Hoadley, C. M. & Kilner, P. G., "Using Technology to Transform Communities of Practice into Knowledge-Building Communities," SIGGROUP Bulletin, January 2005, Vol. 25, No. 1.
16. Chen, et.al, "Systems Requirements for Organizational Learning," Communications of the ACM, December 2003/Vol. 46, No. 12
17. McNurlin & Sprague, Information Systems Management in Practice, Pearson Education, Inc. 2006
18. Michelman, "Why Voting?" Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 985-1004
19. Cain, "Internet Voting in the (Dis) Service of Democracy?" Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1005-1021
20. Nockelby, "Why Internet Voting?" Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1023-1031
21. Grove, J., "ACM Statement on Voting Systems," Communications of the ACM, October 2004, Vol. 47 No. 10.

22. Morris, "Direct Democracy and the Internet," Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1033-1053
23. Garrett, "Political Intermediaries and the Internet 'Revolution,'" Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1055-1069
24. Schwartz, "Vote.com and Internet Politics: A Comment on Dick Morris' Version of Internet Democracy," Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1071-1087
25. Moglen & Karlan, "The Soul of a New Political Machine: the Online, the Color Line, and Internet Democracy," Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1089-1115
26. Kang, "E-Racing E-Lections," Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1155-1170
27. Pershing, "The Voting Rights Act in the Internet Age: an Equal Access Theory for Interesting Times," Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1171-1212
28. Volokh, "How Might Cyberspace Change American Politics?" Loyola of Los Angeles Law Review, Symposium on Internet Voting and Democracy, April 2001, Vol. 34, No. 3, pp. 1213-1221
29. Hoffman, "Diebold's Problems Worse Than Reported, Tests Find," VerifiedVotingFoundation.org, August 3, 2005, http://www.verifiedvotingfoundation.org/article.php?id=6257
30. Gedan, "Rhode Island: Paper vs. Scanner: Ensuring the Vote's Integrity," The Providence Journal, December 3, 2006
31. Anonymous, "Requiring Software Independence in VVSG2007: STS Recommendations for the TGDC," December 1, 2006, http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf
32. Rivest, R. L. & Wack, J. P., "On the Notion of 'Software Independence' in Voting Systems," July 28, 2006, http://vote.nist.gov/SI-in-voting.pdf
33. Dill, "NIST Reaches Unavoidable Conclusion: Paperless DRE's Not Acceptable," November 30, 2006, http://www.verifiedvotingfoundation.org/article.php?id=6426
34. Simons, B., "The Good, the Bad, and the Stupid," ACM Queue, October 2004, pp. 20-26
35. "The Open Voting Consortium," http://www.openvotingconsortium.org
36. Vora, P., "David Chaum's Voter Verification Using Encrypted Paper Receipts," http://www.seas.gwu.edu/~poorvi/Chaum/chaum.pdf.
37. Mercuri, R., "Electronic Voting," http://www.notablesoftware.com/evote.html, September 1, 2005
38. Xenakis, A. & Macintosh, A., "E-electoral Administration: Organizing Lessons Learned from the Deployment of E-voting in the UK," International Teledemocracy Center, 2005, http://diggov.org/library/library/dgo2005/e_voting/xenakis_e_electoral.pdf

About the author

Tim W. McGraw is a graduate student in the Masters of Strategic Technology Management at Marist College in Poughkeepsie NY. He holds an AB in computer science from Vassar College, an AS in Liberal Arts from Dutchess Community College, and has held systems positions including administration and analysis. Tim has experience in finance, education and internet commerce.