# Voting Equipment and Ballots

Stephen Ansolabehere[1]
Ronald Rivest[2]
September 2013[3]

Voting machine failures stood front and center in the recount of the 2000 presidential election vote in Florida. The election dispute between George Bush and Al Gore exposed problems in the absentee and registration systems, in the management of polling places, and even in the definition of a vote in Florida's law. However, a single image captured the heart of the election controversy: Judge Robert Rosenberg of Broward County Canvassing Board inspecting punch-card ballots with a magnifying glass to determine whether the card indicated a vote for Bush, a vote for Gore, or one of the many ambiguous hanging, dangling, or pregnant chads. The technology for recording and tabulating votes had failed, plain and simple, and the determination of the Presidential election hung in the balance. In an age of ever-greater computing innovations and power, America was still using 1960s computer technology — punch-cards — to vote. Surely, there was a better, more reliable way.

That was the starting point of the collaboration between Caltech and MIT: to find a better way to cast and count votes. As it turned out, that was not a hard problem. One could certainly build a better machine than the punch-card systems used in many Florida counties in 2000, and indeed, many companies already had developed technologies such as optical-scan paper ballots and electronic machines with touch-screen interfaces. The biggest problem was that improved voting systems just were not being used widely.

A visit to the proceedings of the Florida Governor's Task Force on Election Reform in January 2001 revealed why. Confusion reigned as a dozen voting machine vendors attempted to persuade the commission to adopt their machines. For their part, the task force members lacked information about the performance of the various technologies in actual elections, and they had no background in matters such as computer security or technology standards. The task force also faced strong opposition to any statewide actions from the state's 67 county election officials, each a constitutionally elected officer in Florida. We shared what we had learned to that point about the reliability of voting equipment — namely, that optical-scan and

---

[1] Professor of Government, Harvard University.
[2] Andrew and Erna Viterbi Professor of Computer Science, MIT.
[3] This report is a slightly revised version of our contribution to Caltech/MIT Voting Technology Project, *Voting: What Has Changed, What Hasn't, and What Needs Improvement.* September 24, 2012. http://vote.caltech.edu/content/voting-what-has-changed-what-hasnt-what-needs-improvement. All references are contained in that report.

electronic equipment produced fewer uncounted votes on average than punch-cards. But, it was evident that the problems facing state and county election officials went deeper than the need for a new type of voting machine.

The voting machine challenge has four components. First, equipment must be reliable. Second, voting machines need to be secure. Third, there must be standards for performance in order to assist governments in making appropriate decisions. Fourth, and perhaps most important, there needs to be a sustainable business model for the voting machine industry.

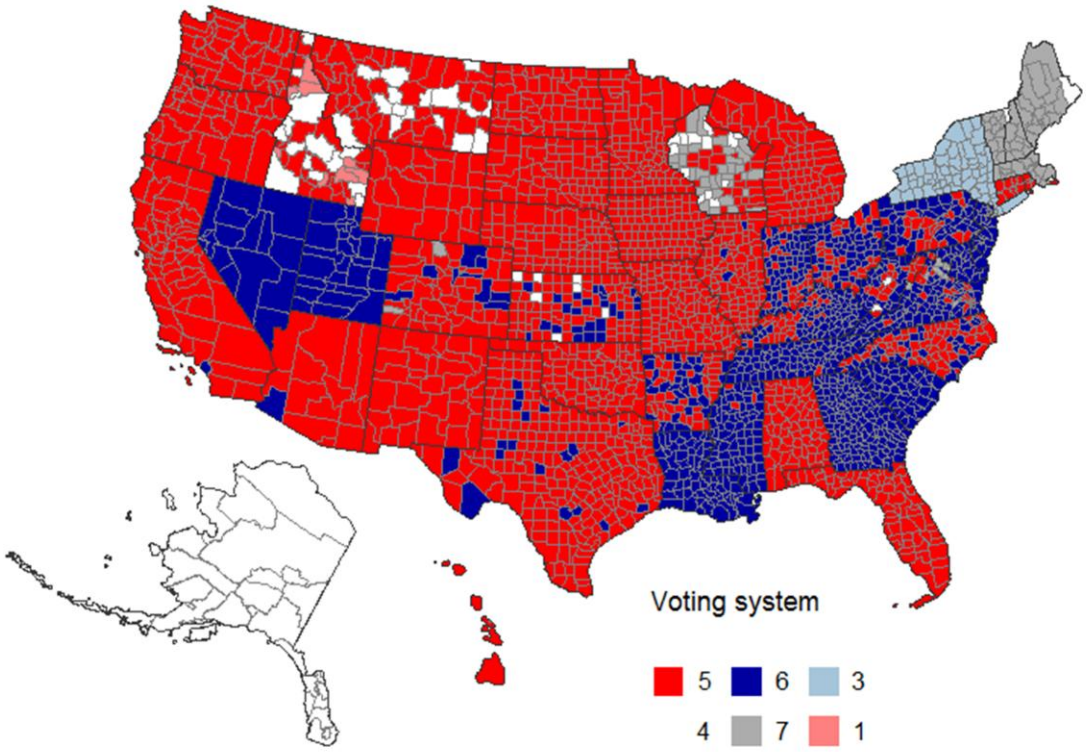
## What has happened since 2000

County and state governments in 2001 needed an immediate solution to the voting equipment vulnerabilities exposed in Florida. It was evident to us at the time that the choices available for adoption before the 2002 (or even 2004) elections consisted of machines already on the market. By the time technology firms could develop, certify, license and manufacture new equipment, the 2002 election would be over. It was also evident that there was a lack of credible and objective information about the performance of different types of equipment in operation.

In January 2001, we conducted a nationwide assessment on the performance of available voting technology in past elections. That assessment led to several simple conclusions and straightforward recommendations. County and state governments then using punch-card or lever machine voting equipment should decommission that equipment and adopt either optically scanned paper ballots, preferably counted at the precincts, or direct recording electronic voting equipment (DREs, similar to automated teller machines). While these technologies may present other problems, they had a track record of improved reliability in recording and tabulating votes.

The recommendation to replace underperforming or antiquated machines was central to our 2001 report, *Voting: What Is, What Could Be*. It was adopted by Carter-Ford Commission, and it became one of the core provisions of HAVA. In 2000, counties used a wide mix of technologies, including hand-counted paper ballots (in 1% of counties), lever machines, punch-cards, optically scanned paper ballots, and electronic voting machines. By 2006, with the exception of New York State, all punch-card and lever voting machines in the United States had been replaced with optical scan or electronic voting equipment. Today, approximately three out of every five counties use optical-scan technology and two out of five use electronic equipment, and a very small number continues to use hand counted paper.

Voting Equipment Used by Counties in 2008




Source: Election Data Services.

Red: Optical Scan
Dark Blue: DRE
Light Blue: Lever
Gray: Mixed
White: Paper
Pink: Punch Card

As important as our recommendation was for near-term technology improvement, our methodology for assessing voting technology performance and reliability was even more so. In 2000, there was no means for measuring the reliability of equipment for recording and tabulating votes during *actual* elections. The Florida recount guided our thinking. The key problem revealed with punch-card technologies was the large number of ballots on which the voter had attempted to express a preference, but where the voter's preference could not be discerned. That is, some voters went to the polls, received a ballot, marked the ballot, and submitted it. Some skipped voting for president intentionally; and some skipped the office unintentionally, but some attempted to cast a vote but failed.

The difference between the number of ballots cast in an election and the number of votes cast for any office could be used to measure technology performance. The discrepancy between the number of ballots cast and the number of votes counted for any office we termed the *residual votes* for that office. Whatever the reason for the blanked or spoiled ballots, their frequency ought not be correlated with the type of technology used. The correlation between some voting technologies and higher numbers of blanked or spoiled ballots showed the extent to which those technologies offered lower reliability in facilitating voting and counting votes. The residual vote rate for president in 2000 was approximately 2% of all ballots cast nationwide. We estimated that simply replacing older technologies with newer technologies would cut that rate in half (Ansolabehere and Stewart 2005). Our subsequent analyses documented that the improvement to the performance of voting equipment following the full implementation of the HAVA requirements matched our expectations. The residual vote rate reached 1% in 2006 and 2008 (Stewart 2009).

Technology upgrades bought short-term improvements. But other problems of performance and usability remained, in particular, for certain communities of voters, such as those with low literacy or who are blind. The VTP's 2001 report also called for long-term innovation in methods for recording votes; subsequent research led to the development of audio voting and other technologies (Selker 2006). Some technology firms have implemented these ideas; but sustained innovation, we think, calls for an entirely different framework for improving voting technology.

Our 2001 report *Voting: What Is, What Could Be* supported the separation of the development of the user interface from the development of the other components of the system, especially the vote tabulator. Such a separation would allow for continued improvement in the user interface to make voting easier and more universally accessible without forcing equipment vendors and governments to start from scratch in developing the voting system's security, gaining certification, and vending wholly new equipment. That approach, dubbed FROGS, would also accommodate many different methods for voting, but it has not been embraced by

the U.S. industry.[4] The FROGS framework remains an alternative approach to voting technology development that would allow for continued improvement. The increased use of absentee voting and early voting has created new technology needs and problems, as discussed elsewhere in this report. It is worth noting that a few states, such as Virginia, allow submission of absentee ballots for military personnel over the Internet, but security concerns motivate many states to use the Internet for downloading blank ballots that are printed and returned by postal mail.

### Business Model Issues

In 2001, the VTP concluded that the greatest challenge in the future of voting equipment was not the performance of particular machines or the security of the system, but the business model of the industry.

Voting technology is computing and information technology. It involves capturing people's preferences, and aggregating that information into a certifiable vote tally. The United States leads the world in computing and information technology. Yet none of the great American computing and information firms develops or sells voting equipment. IBM, Dell, Apple, Hewlett-Packard have all steered clear of this industry, as have firms that contract information services to other government functions, such as Unisys and TRW. The firms in this industry are highly specialized, providing voting equipment and little else. The industry totals only about $300 million in revenue annually.

The voting equipment industry in 2000 was built on an equipment vendor model. Individual firms would develop a particular technology, the specification of which was protected by trade secrets. Technology was not generally licensed to other firms as intellectual property. The firms would then submit their equipment for testing and certification. Once a machine was approved for use in a state, vendors would then attempt to sell their equipment to individual counties, usually in response to a county's Request for Proposals. Some firms provided service contracts through their local vendors. Some counties had staff on hand to perform service and maintenance, especially for lever machines and punch-card equipment. Much of the effort and investment of the voting machine industry were devoted to its sales force. With more than 8,000 county and municipal election offices, the industry was focused on their needs and maintaining relationships with users and potential adopters of the equipment that a given firm vended. In 2000, there were many small firms in the industry, but four midsize firms had most of the market.

The challenges to sustaining a healthy and innovative voting machine industry at that time were four-fold. First, selling stand-alone equipment made the market very thin. Most counties treated voting equipment as durable goods that will last many years. Second, there were few economies of scale, creating little incentive for

[4] The ES&S Automark is a notable exception; it uses auditable paper ballots. The Brazilian voting equipment vendor Diebold-ProComp has similarly implemented such a system.

entrants. The practice of vending to counties fragmented the market. Third, the counties bore the entire cost to the system. Counties have the fewest resources, but state, federal, and special districts account for nearly all the elections on the ballot. Tensions between the states and counties made for little or no cost -sharing. Fourth, there was little vertical integration. Voting equipment was divorced from the rest of the system, such as registration and software services. Much of this remains true today, but there have been some important changes

In our 2001 report, we recommended several innovations in this market, both from the firm's side and from the government's side. Changes on the government's side were perhaps easiest to effect:

- An immediate infusion of federal funds to pay for the immediate upgrade in equipment.
- Contracting on a larger scale — states or clusters of states, rather than counties.
- Cost-sharing, perhaps on a per election basis.
- Leasing equipment rather than making durable-goods purchases. This seemed particularly important, given the rapid obsolescence of computers.
- New contracting models, along the lines of that adopted in Brazil.

Changes in the industry were more difficult to specify or to implement. We envisioned a radically different technology platform that could allow for certification and transparency in the security side of the equipment and that would allow for rapid and separate development of the user interface. Specifically, we envisioned separating the tabulation and vote storage function from the user interface, which records the votes. The tabulator could then be developed and certified to have a high level of security; the interface could be allowed to develop to reflect rapidly changing technologies of communication. An example (due to Jehoshua Bruck) is a ballot printed with a two-dimensional bar code recording the votes of the person (not unlike on an electronic boarding pass). The ballot can be prepared on any computer and printed anywhere (at the polling place, at a library, at home). The individual voter brings the ballot into the voting booth and it is scanned and stored in a secure bin. [This was termed the FROG in the 2001 Caltech/MIT report Voting: What Is, What Could Be.]

That technology platform was envisioned as one that would fundamentally change the business model surrounding voting and, at the same time, address some of the difficult problems of developing standards for secure voting. Appropriate standards and cryptographic solutions could be implemented for the tabulators; new interfaces for a wide range of users could be quickly brought on line to reflect the latest innovations in devices. Such a technology platform, we argued, would allay security concerns and, simultaneously, open the market to more entrants and more innovation, allowing for rapid improvements in usability.

We also saw that there should be integration of voting equipment with other sorts of election systems, such as registration and election management software. Because registration and election management represent much larger markets (in terms of revenue) we saw those as the potential drivers of a more profitable and robust voting technology industry.

What has changed since 2000? In many respects, there have been profound changes in the voting equipment business, but in some very important respects, very little about this business has changed. Perhaps the most important shift has been the increased involvement of state governments in contracting. Since 2000 we have seen the emergence of some economies of scale in this industry, as many states have adopted statewide contracting. Some neighboring states have even taken the next step of making multi-state contracting arrangements. No states, however, have gone as far as the national government of Brazil and committed the resources to regular upgrades of equipment that meets the state's own technology specifications (rather than the voting industry's own standards and specification). We see this as an eventual step in the natural progression of this business.

An equally important change in this industry was the infusion of federal funds under HAVA for adoption of new equipment or innovations in other technologies. Most states used these funds to get rid of underperforming technologies. Some states have shepherded these funds to devote to long-term development of registration software and future equipment purchases. The HAVA money created a bridge for many counties and states between older technologies, especially punch-cards and lever machines, which were increasingly impossible to maintain and use, and new technologies. The problem (as discussed below) will be the next transition, as the HAVA funds were a one-time commitment, rather than an ongoing cost-sharing arrangement.

The advent of statewide contracting transformed the government side of the voting machine business, but the basic business model remains the same. The industry is still based on developing, certifying, and selling stand-alone machines. Ten years after the passage of HAVA, the industry remains the same size (in terms of total revenue) as it was in 2000. After the commitment of the HAVA funds, total revenues of all voting equipment firms sank back to $300 million annually. There has been relatively little effort to integrate the voter registration software and services business with the voting equipment business.

The structure of the industry has changed somewhat, but not necessarily in ways that will produce technological innovations. One firm, Election Systems & Software (ES&S), now controls a large share of the market. In 2009, ES&S had arranged to purchase Premier (the new name for what had been Diebold Election Systems). The Department of Justice filed an antitrust suit. ES&S controlled 47% of all installed machines in 2008 and had $149.4 million in revenues. Premier, the second largest firm in the industry at the time, accounted for 23% of all installed machines and $88.3 million in revenue. Combined, ES&S and Premier would have more than 70%

of the installed equipment and industry revenues. The agreement reached with ES&S allows further consolidation of the vendors in this market.

Meanwhile, firms in closely related fields, such as American Cash Register, Unisys, or Hewlett-Packard, have stayed out. The story of Diebold (see below) is emblematic of the industry's problems. Diebold is, by far, the largest firm to have entered the U.S. voting equipment business over the past decade. The low revenue, high cost, and bad publicity of the American voting equipment market did not make this a lucrative business for Diebold. It shed its U.S. voting equipment division within six years of acquisition.[5] The nature of contracting offers the economy of scale needed to make voting machine production viable on a large scale and to attract large companies, which either avoid the U.S. market altogether or are driven out after brief flirtations.

There has, however, been no radical transformation in the basic technology platform of voting. It remains pretty much what it was in 2000, though there have been experiments in other countries (such as Brazil) to would implement the technology architecture envisioned.

## Security Issues and Technology Innovations

The 2000 United States presidential election put a spotlight on the fragility and vulnerability of voting technology. It became clear that providing robust, accurate, and secure voting systems remained an important open technical problem. In response, Congress passed the HAVA Act of 2002, presuming that the states could solve this problem with a combination of increased funding and the guidance of the newly created Election Assistance Commission (EAC) and its advisory committee, the Technical Guidelines Development Committee (TGDC).

Spending money on a problem works best for well-understood problems, such as building roads or fixing bridges. How secure and reliable voting systems should be designed and configured was, and still is, only partially understood. To spend funds wisely on new voting systems requires patience, and significant research and development. Congress gave funds to the states immediately, so the states bought large numbers of voting systems that were then available. Those systems remain in place, and they reflect the security protocols and standards at that time (2000).

### *Signs of trouble—Security Revelations since 2000*

We begin with a brief overview of two narratives that illustrate the problems with voting systems purchased during the first decade of the 21st century: the saga of Diebold, and the investigations by the state of California. These are only

[5] Diebold remains interested and active in the voting equipment industry, but not in the U. S. Diebold purchased ProComp of Brazil in 1999, and is the primary vendor of voting technology to the entire nation of Brazil.

representative threads; details can be found in books by Alvarez and Hall (2008) and Jones and Simons (2012).

*Diebold investigations*. The Diebold saga is instructive, showing how the existing process of developing, certifying, and purchasing voting systems failed to provide systems meeting even minimal criteria for security.

Diebold is an old and well-respected company, known for producing safes, bank vaults, and — more recently — ATMs. In 2002, it entered the business of voting systems with the purchase of Global Election Systems. While this looked like a good direction for Diebold's growth, subsequent events showed that Diebold failed to follow through by ensuring that the voting systems sold under its name were well-engineered. In the end, Diebold sold off its voting systems division to ES&S in 2009. (ES&S was required the next year by the U.S. Department of Justice to divest this purchase, which it did by selling it to Dominion Voting Systems).

The Diebold systems were "DREs" — voting systems using "direct recording by electronics." These systems had no paper records; *all* information was processed and stored electronically. Such designs were typical of the times. But all-electronic "Black-box" voting means a voter has no way of verifying that the voting system is recording his or her votes correctly — the machine could be displaying one candidate's name on the screen while mistakenly or maliciously storing another candidate's name on the official electronic record as the voter's choice.

In 2003 Bev Harris, a well-known voting-integrity activist, author of the book "Black Box Voting" (Harris, 2004) and founder of BlackBoxVoting.org, announced that she had obtained software for Diebold voting machines from a non-secure Diebold website. A number of teams examined the Diebold voting system software, including Science Applications International Corp. (SAIC), which was commissioned by the state of Maryland in 2003 to do so. SAIC issued a report (SAIC, 2003) that found that, although no overtly malicious code was found, the system was so poorly engineered that it exhibited a "high risk of compromise." A study of the software discovered egregious security lapses, such as the fact every Diebold voting system used the same "secret" encryption key, effectively making the encryption useless (Kohno et al. 2004).

A flood of other studies followed.[6] All were withering in their denunciation of the systems' security; some — such as studies by Hursti and by Felten — showed how the machines could be controlled by malicious parties and infected by viruses.

[6] Among these studies were those by Compuware (2003), RABA (2004), Professor Ed Felten and his Princeton students (Feldman et al., 2007), Harri Hursti (2006), the 2007 studies by the state of California in its Top-To-Bottom Review (California Secretary of State Debra Bowen 2007) and the state of Ohio in its EVEREST report (Ohio Secretary of State, 2007).

In the context of the revelations about Diebold voting systems, and given the weak federal certification program for voting systems, individual states began to respond by sponsoring more rigorous examination of their existing voting systems.

California was a leader. In 2007, California Secretary of State Debra Bowen established the Top-to-Bottom Review (TTBR) of all electronic voting systems; high-caliber teams of experts were contracted to perform a thorough (but brisk) review. In July 2007, Bowen decertified all the DRE systems, with conditional recertification if the companies provided improved security features and if the counties followed certain post-election auditing procedures to ensure that the machines were returning the correct results. Her decisions favored systems based on the optical scan of paper ballots, as they are "more transparent, and significantly easier to audit."[7]

### *Technical proposals for security improvements*

Since 2000, there has been an extensive study of voting from a security perspective. Three themes stand out: the need for software independence, the necessity of evaluating end-to-end voting systems, and requirements for post-election auditing. All three relate to increasing the verifiability of election outcomes.

*Software independence*. The notion of "software independence" (Rivest and Wack , 2006, and Rivest 2008) captures the intuition that election outcomes should not be critically dependent on software-based voting systems. More precisely, a voting system is said to be "software independent" if a (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome. This notion was proposed for adoption as part of the federal voting system certification standards (the 2005 Voluntary Voting System Guidelines). The notion does not exclude the use of software, but recognizes the extraordinary difficulty of producing correct software, by requiring that election outcomes produced by software-based voting systems be checkable by other means; the simplest software-independent approach is to complement such systems with voter-verifiable paper ballots.

*End-to-end voting systems*. An "end-to-end" (E2E) voting system provides verifiability from the starting point (the choices in the voter's mind) to the final tally. Votes should be verifiably (by the voter) cast as intended, verifiably (again by the voter) recorded as cast, and verifiably (by anyone) tallied as recorded. Overall, this provides a level of verification of the election outcome that exceeds what is available in voting systems in current widespread use.

There have been numerous proposals for E2E voting systems; we mention only two here. They typically involve the use of cryptography and also a website where

[7] https://josephhall.org/nqb2/index.php/casosttbrstmt

voters can check that their (encrypted) votes are correctly logged. Checking that encrypting ballots is properly performed and checking that the tally of the encrypted ballots is correct are typically non-trivial but doable.

The "Prêt à Voter" system (Chaum et al. 2005) is an E2E voting system using a two-part paper ballot, with one part containing the candidate names (in scrambled order), and the other part containing the voter's choices and some encoding of the name permutation. The voter casts only the second part, and discards the first part. See Peter Ryan's "Perspectives'' piece in the 2012 Caltech/MIT Voting Technology Project Report.[8]

The "Scantegrity'' system (Carback et al. 2010) uses an innovative invisible-ink method on what appear to be ordinary optical-scan paper ballots. However, when the voter marks a bubble (using a special pen) a secret "confirmation code'' is revealed. The voter can look up these codes on a website later to confirm that his ballot was properly recorded. The Scantegrity system has been successfully used in two binding governmental elections, in Takoma Park, Maryland.

*Election Auditing*. Election audits are an effective approach to verifying the correctness of election outcomes (e.g., Alvarez, Atkeson, and Hall 2012). Some such audits assume that the paper ballots being counted have not been tampered with, but more holistic audits involve auditing the election process end to end, to ensure that all ballots can be accounted for throughout the election process. Such systems function largely through effective standard operating procedures (Alvarez and Hall 2008), which help to ensure that mistakes are not made in the handling of ballots (either electronic or paper). Such comprehensive audits resemble, in certain respects, E2E systems, which make no assumptions about ballot authenticity and provide for detection of tampering via the website.

A post-election audit verifies the correctness of the reported election outcome by hand-counting a sufficiently large random sample of the cast paper ballots. (Here "correctness'' refers to the agreement of the announced election outcome with the outcome that a full hand-count would provide; the audit checks the correctness of the machine-counting of the paper ballots.) The sample may either sample precincts or single ballots; the latter can be noticeably more efficient. A statewide election for a large state may be audited by examining just a few hundred ballots, for a typical margin of victory. If the margin of victory is small, or if the originally reported outcome was incorrect, the audit may escalate, auditing more and more ballots, until a sufficient level of statistical confidence is established. For a typical large election, only a tiny fraction of the ballots need to be examined.

---

[8] Caltech/MIT Voting Technology Project, *Voting: What Has Changed, What Hasn't, and What Needs Improvement.* September 24, 2012. http://vote.caltech.edu/content/voting-what-has-changed-what-hasnt-what-needs-improvement.

Since 2000, the technology for post-election audits has improved greatly. Professor Philip Stark (U.C. Berkeley) has pioneered many of the new techniques; his website[9] includes many key papers. One new method is the "risk-limiting audit," which guarantees with high probability that if the originally reported outcome was incorrect, the audit will not terminate until all the ballots have been examined. The audit has a bounded probability (the "risk-limit") of confirming an incorrect outcome. Other post-election audit methods, such as the "Bayes audit" (Rivest and Shen 2012), have somewhat similar properties.

At least half of the states will be conducting post-election audits (Verified Voting, 2012). Some are running pilot risk-limiting audits; California has run more than 20 such pilots under its program initiated with the 2010 Assembly Bill 2023 (California Secretary of State 2011-2012).

Election auditing can be a powerful tool for assuring the integrity of election outcomes. Audits can be quite inexpensive to run, and can decrease the need for costly certification of voting systems.

These innovations are promising, and other researchers have proposed still other technological solutions for improving security and usability of electronic voting equipment. One important challenge though is getting new technologies to market in a timely manner. Certification is expensive and time consuming, making it difficult to adopt innovative technologies that improve on existing equipment.

### *Innovations and Change*

Over the past decade, we have seen the following trends in voting system security:

- A strong movement away from all-electronic voting systems, toward voting systems based on paper ballots.
- Increased interest in post-election auditing.
- Strong interest from computer security experts and cryptographers in the problems of voting system security.
- Some jurisdictions (such as Travis County, Texas) taking the design of voting systems into their own hands, in consultation with expert advisory boards.

On the other hand, the following are trends that may weaken security of voting systems:

- Apparent increased interest in vote-by-mail and Internet voting. (In general, remote voting has much increased risk of vote-selling and voter coercion.)
- The federal certification system seems largely dysfunctional at present (discussed below).

[9] http://statistics.berkeley.edu/~stark/Vote/index.htm

- The voting system industry is over-centralized, has little transparency, and invests insufficiently in research and development.

### *Has Security Improved?*

Has the security of voting systems improved since 2000? It is difficult to answer this question because we do not have systematic data that can be used to examine this question over time. Studies of legal prosecutions by the federal government do not suggest that fraud is rampant (Bailey 2008), although case selection and the lack of systematic study does lead us to the old maxim "Absence of evidence is not the same as evidence of absence.''

Researchers have developed over the past decade an array of statistical methodologies for attempting to identify election fraud using statistical methods or natural experiments that arise from election administration (Alvarez et al. 2008; Hill 2006). Mebane illustrates the detection of election fraud by irregularities in the patterns of digits of reported tallies.[10] Hyde's (2007) path-breaking work, for example, examines the incidence of irregularities in counts and their correlation with the placement of U.N. election observers in various new democracies. There are also important studies of individual countries (on Russia and the Ukraine, Myagkov et al. [2009]; on Venezuela see Levin et al. [2009]).

The increased interest in election auditing and in verifiability of election outcomes bodes well for improved security throughout the next decade. There is, however, a clear need for systematic assessment of election fraud. We see the following questions as essential as the area of secure voting systems moves forward.

- To what extent has fraud occurred in previous elections?
- Are voting systems returning the correct election outcome?
- Are voting systems providing good evidence for the correctness of the election outcomes they are reporting? Is the outcome verifiable*?*

### *Recommendations*

We have developed the following recommendations for improved security of voting systems:

- Implement effective election auditing procedures at the local and state levels, which at a minimum would require post-election auditing of all voting technologies used in an election.
- Continued strong support for voting systems security research is critical, emphasizing auditing and the verifiability of election outcomes.
- Continued work is needed examining the role of human factors and standard operating procedures in making elections more secure, including more

[10] http://www-personal.umich.edu/~wmebane/

effective chain-of-custody rules and clarity on security procedures to be used throughout the electoral process.

- Mandated use of public standards (such as EML) is required for representation of data by and between voting systems.[11]
- Mandated ownership of all election data by the electoral jurisdiction is necessary. Vendors must not own the election data.
- Encouragement for continued research into election forensics methods is required, as well as the collection and distribution of data necessary for their application in the immediate aftermath of contested elections.

## Standards Development

Although the National Commission on Federal Election Reform's Task Force on the Constitutional Law and Federal Election Law noted that Congress does have the constitutional power to regulate federal elections, it has not historically done so. Instead, the federal government has historically deferred to the states the regulation of elections, and this "states rights'' posture means that effective federal regulation of the voting system industry is not direct, but indirect, through pressure and payments made by the federal government to the states. Effective federal regulation only works with the voluntary cooperation of the states. However, with the passage of the Help America Vote Act (HAVA) of 2002, some advances were made concerning the adoption of voluntary voting system standards.

This section briefly reviews the pre-2002 standards landscape, examines the effect of HAVA 2002 on regulation and voting systems standards, and, finally, makes some recommendations for improvements.

### *Early standards (pre-2002)*

Prior to 2002, the only federal standards for voting systems were those adopted in 1990 by the Federal Elections Commission. The standards were created after the publication of several major reports about issues related to voting technology (Saltman 1975; Saltman 1988) by Roy Saltman of the National Bureau of Standards (now NIST, the National Institute of Standards and Technology) and after some activity at the state level in this area (Federal Elections Commission 1990). These standards were voluntary, and no corresponding testing process existed until 1994, when the National Association of State Election Directors (NASED) created one. At that point, some states began to require conformance to these (voluntary) federal standards; by 2001 a majority of the states had done so.

While the adoption of these voluntary standards was a significant first step, there were major gaps, weaknesses, and problematic aspects. For example, the voting system vendors directly paid Independent Testing Authorities (ITAs) for the

[11] http://en.wikipedia.org/wiki/Election_Markup_Language

required testing, an arrangement with a clear potential for conflicts of interest. The handling of the security of voting systems was very narrow and limited; for example, there was an exemption of Commercial Off-The-Shelf components (COTS components) from examination, even if these components were integral to the system. Neither voters, nor pollworkers, were included in the testing. NASED adopted a revised set of standards in 2002, just before the passage of HAVA, but these standards had similar weaknesses.

### *HAVA 2002, the EAC, and the TGDC*

The Help America Vote Act of 2002 provided substantial funding — more than $3 billion — to the states to improve their voting systems, with primary goals of replacing outdated punch-card and lever machines. The Act also set up a process for developing improved voting system standards.

HAVA established the Election Assistance Commission (EAC) to oversee and administer these improvements, as well as a Technical Guidelines Development Committee (TGDC) to develop the next round(s) of the Voluntary Voting System Guidelines, to replace the NASED 2002 standard.

The technical work of developing standards was to be performed by the Technical Guidelines Development Committee (TGDC), comprising 15 members from designated areas. The National Institute of Standards and Technology (NIST) provided strong technical and editorial support to the TGDC.

NIST held a meeting in December 2003, titled "Building Trust and Confidence in Voting Systems" to allow many stakeholders to express their views on what ought to go into a new standard. The most contentious issue was that of paper versus electronic ballots. One critical debate that the TGDC had to navigate was one between those who strongly support electronic systems because they allow individuals with disabilities the opportunity to cast ballots without assistance and those who are concerned about the auditability and security of electronic voting technologies.

The TGDC started work in 2004, and by December 2005 had its first set of Voluntary Voting System Guidelines approved; these guidelines went into effect December 2007. These initial guidelines were a modest rewrite of the NASED 2002 standards. The TGDC continued its work, and in August 2007 provided a substantial rewrite of the proposed Voluntary Voting System Guidelines. A notable feature of this rewrite was the requirement for "software independence" — the requirement that a software error could not cause an undetectable error in an election outcome. This requirement effectively means that the operations of software-based voting systems need to be auditable. The TGDC determined that this requirement is met by the use of paper ballots, as paper ballots can always be recounted by hand if desired, thus providing the necessary detectability of software errors.

The EAC has not approved the VVSG 2007 proposed guidelines, in part due to opposition to the requirement for software independence. Some opposition to the entire standards process has been bubbling up within NASS (the National Association of Secretaries of State), including a motion in favor of eliminating the EAC altogether.

### *What are federal standards good for?*

Voting system standards are useful for examining the basic functionality, usability, reliability, and elementary security aspects of voting machines.

However, there are several conflicts that have become apparent in recent years regarding voting systems standards in the U.S.:

- Federal standards versus state standards for voting systems.
- A requirement for auditability, (say via paper ballots) versus allowing unauditable but potentially more flexible and user-friendly DREs.
- Requirements for voting systems for voters with disabilities versus general voting system requirements.
- The expense of having voting systems certified and the need for innovation.
- A desire for high integrity in voting systems versus the fact that testing and certification cannot ensure secure voting systems. Note that security is a negative quality. You can test that a voting machine weighs at most 80 pounds, but you cannot test that a voting machine is "secure."

In a recent paper, Stark and Wagner (2012) argue that a better approach is to audit election *outcomes* (via post-election audits) than it is to try to ensure accurate election outcomes via testing and certification of election *equipment*.
It is worth noting that certification of voting equipment doesn't protect one from bad ballot design or misprogramming of ballot scanners. Even the best-tested equipment can be misused to yield invalid election outcomes; post-election audits are capable of detecting and correcting such problems.

Have federal standards helped improve voting systems in the U.S.? The answer isn't clear. While they may have helped ensure that voting systems meet some basic requirements, the difficulty, cost, and time involved in having voting systems certified have certainly also made life difficult for new voting system vendors and election officials. Certification costs and delays are often raised by vendors and experts as a factor that slows the evolution of technology or prevents the adoption of a new technology platform.

### *Recommendations*

We propose the following recommendations regarding standards for voting systems:

- De-emphasize standards for security, aside from requirements for voter privacy and for auditability of election outcomes. While testing for minimal security properties is fine, expecting ITAs to do a thorough security review is unrealistic and not likely to be effective. Instead, statistically meaningful post-election auditing should be mandated. ("Audit the election outcome, not the election equipment" (Stark and Wagner 2012)).
- States should harmonize their voting system requirements; right now the market remains highly fragmented, in part because different states have different requirements. Harmonization would help reduce costs, especially if accompanied by increased information sharing on best practices and common problems.

### Voter Intent

Largely unstudied since 2000 are standards relating to assessing voter intent. When we look back at the 2000 election in Florida, it is important to remember that Judge Robert Rosenberg of the Broward County Canvassing Board was not just dealing with the results of an antiquated voting technology when he looked through the magnifying glass at the punch-card in this famous photo. He was also attempting to determine what those ballots said about the intent of the voters who marked them. A subject for concern with the return to paper ballots in many states is the ability of election officials to ensure a clear understanding of the intent of the voter.

The issue of voter intent has come to the fore in two recent elections in Minnesota. In both 2008 and 2010, the closeness of the election resulted in some ballots being scrutinized to determine if the votes were for one candidate or the other. In 2008, this process took eight months — a time frame that would not have been possible in a presidential election, when electors have to be chosen approximately seven weeks after the election.

If a state does not have clear standards for what constitutes a vote on a paper ballot — for example, stating that underlining or circling a name is the same as marking the oval next to the candidate that can be read by an optical scanner but that writing in the name of a candidate on the write-in line after also filling in the oval is an overvote — then problems like Florida can happen again even with new voting technologies.

States should review their standards for voter intent, and insure that they remain clear, unambiguous, and up-to-date as voting technologies continue to evolve. Standard-setting organizations should develop best practices for voter-intent standards, with the assistance of election officials and the research community.

### Looking Forward

We see several near-term challenges and opportunities over the coming decade.

- States, counties, and municipalities will need to upgrade technologies within the next few years. Most of the electronic voting equipment in place today was developed and certified in the first half of the 2000s, or earlier. Simple obsolescence of computer hardware and operating systems will require an upgrade. This is a significant problem, but also a big opportunity.
- There is a shortage of technology options. Currently certified voting technology often does not reflect recent innovations in voting or computing technology, because of the slowness and expense of the certification. There is a need to bring in new ideas and approaches, but the process for technology adoption creates significant barriers.
- Adoption of Internet voting will continue. Vendors and jurisdictions will continue to propose a variety of ways to cast votes over the Internet, despite the security challenges. However, the Internet will be increasingly used to transmit blank ballots to remote voters, who can print them out, indicate their choices on the printed ballots, and return them via postal mail.
- There will be increased levels of experimentation with, and adoption of, post-election auditing; strong support for auditable voting systems via federal or state standards; and possible adjustment of election calendars to better accommodate post-election audits.
- State election administrators will take on an increased role of leadership and authority relative to federal and local administration because of changes in equipment purchasing and certification. That will result in increased state-level centralization of information, and more states adopting statewide voting systems.
- Computerization of election administration will continue to proceed, with increased attention on the access to, accuracy of, and security of voting registration systems, and on the development of tools to improve management of elections.

## References

All references are contained in Caltech/MIT Voting Technology Project, *Voting: What Has Changed, What Hasn't, and What Needs Improvement.* September 24, 2012. http://vote.caltech.edu/content/voting-what-has-changed-what-hasnt-what-needs-improvement.