2009

Voting and Registration Technology Issues: Lessons from 2008

S. Candice Hoke
Cleveland State University, s.hoke@csuohio.edu

David Jefferson

Original Citation

Candice Hoke and David Jefferson, Voting and Registration Technology Issues: Lessons from 2008, in America Votes! A Guide to Modern Election Law and Voting Rights [Supplement] 37-64 (B. E. Griffith, ed., American Bar Association, 2008)

January 1, 2009

Voting and Registration Technology Issues: Lessons from 2008

S. Candice Hoke, *Cleveland State University*
David Jefferson, *University of California - Davis*

CHAPTER THREE

VOTING AND REGISTRATION TECHNOLOGY ISSUES: LESSONS FROM 2008

CANDICE HOKE AND DAVID JEFFERSON

After the 2000 presidential election exposed flawed technologies for vote recording and tabulation and for maintaining voter registration files,[1] Congress appropriated more than $3 billion in an effort to upgrade these systems nationwide, usually to state-of-the-art, computer-based equipment. The massive Help America Vote Act of 2002 (HAVA)[2] described the functional features the new technologies should attain[3] but did not articulate or provide a process by which any mandatory federal technical standards would issue. Nor did it require a compliance system for ensuring that voting equipment and voter registration systems would satisfy the statutory standards. HAVA did require, however, a relatively rapid timetable for purchase and deployment of the new systems.[4] Underlying this rapid move to computer-based voting and voter registration lay a critically unexamined assumption: technologies (such as automatic tellers and accounting software) used for many years in other industries could be quickly adapted by vendors to bring voting into the twenty-first century. Further, the Act reflected the prevailing congressional belief in the capacity of market forces to produce high-quality products at lower prices than a scheme of mandatory federal regulation.

HAVA created a new federal election administrative agency, the U.S. Election Assistance Commission (EAC),[5] to disburse funds and to implement other sections of the Act that federally mandated new state efforts in election administration. Before HAVA, many states had left election administration within the domain of local officials, who had little state supervision or involvement.[6] Partly from displeasure with the Federal Election Commission's exercise of its regulatory authority,[7] and partly in response to the traditional roles of state governments in conducting elections, Congress generally chose not to delegate to the EAC mandatory regulatory power over election administration.[8] Instead, Congress charged the EAC predominantly with the role of providing "guidance" via "best practices" and "voluntary" standards for state election officials.[9]

Given that by 2008, most local election offices had acquired at least two years' experience with their new voting technologies, some may have tacitly assumed that the voting technology issues of prior years would not resurface in the 2008 presidential cycle. Vendors had previously dismissed technical malfunctions as attributable to human error by poll workers, voters, or election officials,[10] who presumably had learned from prior mistakes. The empirical record that has been generated during the entire 2008 election cycle, however, documents a wide range of technical issues with voting systems, and to a somewhat lesser degree, with the statewide voter-registration databases. When the record is taken as a whole, and in conjunction with the comprehensive, independent scientific assessments,[11] the technical "incidents" that interfere with the conduct of an election are increasingly understood to relate to the equipment's design, its engineering-manufacturing, and its documentation in operational manuals. The issues cannot be attributed simply to operator or human error.

By mid-2007, the federal HAVA disbursements to states had totaled nearly $3 billion in four years.[12] In appropriating these funds, core congressional statutory objectives included improving the voting experience, increasing accessibility for disabled voters,[13] augmenting voter confidence in the democratic process,[14] and reducing the voting machine error rates from the 2 percent average of punch-card systems to a fraction of their former levels.[15] But achievement of each of these objectives appears more elusive as questions of the accuracy, reliability, and security of the current generation of voting systems and of the voter registration databases have become increasingly serious and scientifically documented. The apparent achievement of significantly reduced incidence of balloting errors,[16] particularly "overvotes" and unintended "undervotes," is more questionable when the voting system's performance does not comply with scientific and engineering standards for assuring high accuracy, security, and reliability.

This chapter reviews the 2008 election performance and scientific assessment records of the two major HAVA-promoted election technologies considered here, the voting systems themselves and, to a lesser extent, the statewide voter-registration databases, to delineate both their performance records and the statutory and regulatory apparatus that produced the technological shift. Perhaps surprisingly, HAVA's role in generating each of these election technologies is quite different. While HAVA mandated and constituted the originating impetus for most of the statewide voter-registration database systems that were in use for the 2008 election cycle, and provided major financial incentives for the shift to computer-based voting, HAVA did not generate and was not the source for the regulatory and certification testing apparatus that approved voting systems for 2008 usage. Development and implementation of the HAVA-mandated voting system guidelines and its testing apparatus consumed significant time, effectively leaving in place the prior standards and certifications under the Federal Election Commission.[17]

In searching for the reasons behind national deployment of voting and database technologies whose reliability, security, and other technical properties were profoundly deficient, at least four major reasons can be adduced. First, the HAVA-mandated regulatory activities were not sequenced properly for the best use of the federal monies. Second, the timetable for purchase and initial launch of the technologies was far too ambitious for developing voting equipment that would function at high standards of accuracy, security, and reliability. Third, HAVA dedicated far too little attention to the regulatory, managerial, and technological infrastructure at both the federal and state levels that was needed to support the dramatic systems shift, instead apparently assuming the market would satisfy the technical needs.[18] Fourth, the Act's faith in the market to produce exemplary election equipment was misplaced, especially in light of the rapid pace of procurement and deployment the Act mandated.

I. The 2008 Performance Record of Digital Voting Systems

By 2008 most states had shifted a large proportion of their voters to electronic voting systems, using HAVA funds for new procurements. The new computer-based equipment was designed to generate ballots, record votes, tabulate results, and produce reports of election results.

A. THE SCIENTIFIC ASSESSMENTS OF VOTING SYSTEMS

HAVA funding that states used for replacing punch-card and lever systems could only be expended on voting systems that met minimum statutory criteria for functionality.[19] This set of restrictions led predominantly to purchases of three kinds of systems: (a) optical scanners for reading paper ballots (both the portable, low capacity, precinct-based scanners and the high-speed, high-capacity, centralized scanners), (b) direct recording electronic (DRE) machines that usually feature a touch screen for selecting ballot choices (often conceptualized as an ATM-like voting device), and (c) computerized ballot-marking devices designed primarily for disability access.[20] If a jurisdiction selected paper ballots and scanning systems,[21] then a single technology would suffice for both absentee voting and precinct voting on Election Day, but precincts would also have to be supplied with ballot-marking devices to support the visually impaired. If a jurisdiction chose DRE devices for precinct balloting, the jurisdictions expected it to support both able-bodied and most disabled voters, as vendor marketing suggested.[22] DRE deployment, however, necessitated some additional absentee-balloting technology. Most vendors provide software that helps design digital ballots for both optical scanning and display on DRE devices, and then later tabulates and reports the election totals from both technologies in one omnibus election results report.

The vigorous debate over DRE accuracy, security, and reliability began in 2003 with a report from several prominent computer scientists who are software security experts. They reviewed the source code of a major DRE system (the Diebold TS) that was deployed statewide in both Georgia and Maryland, and also widely in other jurisdictions around the country,[23] identifying numerous serious deficiencies especially related to security. Computers that lack security protections appropriate for their particular application are vulnerable to attacks that can subvert their intended purpose, in this case accurate election results. Attacks on voting systems might render the machines inoperable,[24] or cause them to lose data, or compromise ballot secrecy, or systematically change vote totals in completely undetectable and uncorrectable ways. For this reason computer security experts conclude that security- and mission-critical equipment such as voting systems require "high assurance," i.e., a convincing argument or proof, going beyond simple testing, that the system will *always* do what it is supposed to do *and also* never do what it is not supposed to do.[25]

Following the independent academic report, Maryland commissioned the first of several technical and risk assessments of the same electronic voting system, and other states also initiated voting systems studies of various types. By the 2006 election cycle, at least six major studies had documented a broad range of serious security and reliability deficiencies in systems sold by various vendors.[26] Candidates for Secretary of State in California and Ohio campaigned in part on a promise to initiate closer examinations of their voting systems. In California, newly elected Secretary of State Debra Bowen began planning the independent study of voting systems used in the state immediately after taking office. The new Secretary of State in Ohio, Jennifer Brunner, issued an RFP for a separate study.

Two distinguished computer scientist professors with expertise in both computer security and voting systems led the California "Top to Bottom Review" (TTBR), which the University of California managed. As Secretary Bowen directed, the lead scientists convened four separate teams: software code assessment; "red team"/penetration assessments; documentation review, including of all testing lab reports and vendor manuals; and accessibility assessments. Despite receiving commitments to participate in the TTBR from all four vendors of California-certified voting systems, only three (Sequoia, Diebold (now Premier), and Hart InterCivic) complied with the project's calendar sufficiently to be reviewed. ES&S did not meet the deadline.

The TTBR reports documented a wide range of grave deficiencies in basic security, reliability, accessibility, usability, documentation, and ballot secrecy design and implementation.[27] In later reviews convened in California and also in the Ohio EVEREST risk assessment,[28] the reports documented a similar set of serious deficiencies in the ES&S voting systems using similar criteria.[29] Perhaps the area of greatest concern lay in security, as the vendors had not included high security among the core design criteria, or at least had not achieved it. If security considerations are not included at the design level, post-production corrections are rarely effective.[30]

Some local election officials publicly criticized the voting system studies, arguing that because the security vulnerabilities were identified in a controlled laboratory setting rather than as truly deployed with numerous procedural safeguards in a real election, the conclusions were invalid.[31] By contrast, other officials welcomed the assessments and suggested further efforts.[32]

In 2008, the vast majority of U.S. voters cast their ballots on voting systems designed and marketed by the same four vendors whose voting systems had been shown to be seriously deficient. The uneven performance of these voting systems in real elections was predictable in light of the constellation of technical issues that the published independent studies had documented.

B. THE VOTING SYSTEMS' 2008 PERFORMANCE RECORD

From the inception of the 2008 presidential election cycle, local jurisdictions experienced both apparent successes in using the HAVA-funded voting systems as well as notable calamities. A number of national and local advocacy organizations concerned with election accuracy, often known as "election integrity" groups, assumed the role of citizen technology and security monitors. They communicated voting system technical problems to reporters, questioned election officials at public meetings, and vigorously advocated for auditable voting technology. National research and advocacy nonprofit organizations that focus on technical issues produced major reports.[33] These national organizations, including Common Cause, the Verified Voting Foundation, and the Brennan Center for Justice, published major research and policy recommendations for managing voting technology issues.[34]

With government studies, independent academics, and major research organizations having legitimized the previously dismissed concerns, and with the pressure for riveting stories from the campaign trail, the media became far more active in reporting voting system equipment problems. Because the technical problems were widespread throughout the election cycle, the following review is perforce illustrative rather than exhaustive. In January 2008, South Carolina set the course with malfunctioning DRE touch screens that caused hundreds of primary voters to have to vote on paper towels and other scraps of paper. Officials later identified the cause to be a date programming error that affected voters in two populous counties.[35] Within the same month, several major Florida counties experienced significant interruptions in voting, with reliability issues affecting equipment by the four vendors whose similar (but not identical) voting systems had been evaluated in the California TTBR study. Florida's technical issues included software bugs that impaired vote tabulation accuracy, DRE units that would not boot, memory card and DRE activator card errors, and ballot scanner malfunctions.

On February 5, 2008, and succeeding days, the primary elections on Super Tuesday[36] produced a lengthy list of voting system equipment failures that impeded voting. Several Atlanta polling locations sustained long lines, and some voters departed without voting because the DREs were not functioning. In New Jersey's primary, in some counties using Sequoia Advantage DREs without a voter verification system, election officials discovered a mysterious ballot-counting anomaly. After months of legal wrangling between citizen plaintiffs, the vendor, and the state government, a state court ordered a forensics assessment by computer security scientist Andrew Appel of Princeton University. His research team's October 2008 report concluded that software programming errors were responsible for the anomaly. The team also found that New Jersey's Sequoia Advantage DREs suffered from software and physical security deficiencies similar to those reported in earlier studies of DRE systems.[37]

In advance of the primary election, officials in Sacramento County, California, announced their plan not to use M100 ES&S precinct scanners owing to failures in their logic and accuracy tests. The county moved to a contingency plan, scanning all ballots in the central office. While California's voting technology produced a more positive track record than many other Super Tuesday states, a few counties reported problems with their central count scanners and with memory cards.

Arizona's Cochise County suffered perhaps the most serious tabulation anomaly of Super Tuesday:

> [A]s the county accumulated totals from the precincts, a computer error kept adding the results for five polling places every time new figures were added. The error got worse when the cumulative error went through five updates. County officials noticed the problem when they realized the *total number of ballots cast was reported to be more than the people registered in the county.*[38]

Because the total recorded votes were much higher than expected, election officials noticed and investigated the anomaly. When reporting irregularities are not sufficiently dramatic to draw such attention, however, and routine auditing is not performed, software programming errors that can lead to erroneous election results are unlikely to be identified and corrected. Discovering grave errors by happenstance troubles many advocacy organizations, and they urge the federal Election Assistance Commission to gather and report software errors.[39]

The 2008 general election reinforced the lessons of the primaries regarding the voting systems' uncertain reliability. Under the leadership of the Lawyers' Committee for Civil Rights Under Law, the Election Protection Coalition coordinated more than 100 organizations nationally to field legally trained election observers and troubleshooters. The Coalition established a hotline for voters, poll workers, and others to file reports on election difficulties. Partnering with the Electronic Frontier Foundation, the Coalition also sought to collect and analyze voting equipment problems. While the Coalition did not verify the individual reports and some may not be completely accurate, the constellations of voting system problems tend to match the press-reported technical issues that impeded voting.

Princeton researcher Joe Hall has analyzed the hotline equipment-related call data, finding that "machine breakdowns" led to long lines in numerous locations.[40] In one Atlanta polling place, all 15 DREs were nonfunctional. In other states, precinct ballot scanners failed. Long lines frequently ensued when primary balloting equipment failed, as voters declined to use the back-up balloting systems. Hall reports that voters distrust "contingency balloting" methods; across the nation, when the primary voting system failed, many voters chose to wait several hours for equipment repairs rather than risk having their ballots omitted from the count. Voters also reported to the Coalition hotline that disability access voting equipment was nonfunctional, that it had not been installed and activated when voters arrived, or was not usable in a manner that allowed independent and private voting as required by HAVA.[41] The hotline provided additional data that Hall characterizes as evincing "improper technical fixes" of voting equipment, such as removing voting machines to a parking lot for repairs while voting was occurring.

Of roughly 1,900 voting equipment reports filed with the hotline, Hall found the most frequent was that the voting equipment was "broken" in some manner. These reports included nonfunctional lights, buttons, or legs; unstable screens, failure to boot, or crashing and freezing; failure to properly count or increment the number of ballots; DRE printer jams, DRE vote "flipping," and DRE nonrecording of write-in votes.[42] In the states permitting early in-person voting and increased absentee voting by mail, these innovations mitigated the Election Day demands on finicky equipment and likely rendered more voters able to cast ballots than if voting occurred on only one date.

In the search for the reasons behind computer-based voting systems' problematic performance record in 2008, the trail leads to regulatory decisions and gaps dating to almost 20 years ago. Unfortunately, at the inception of computers in voting systems, Congress did not perceive the substantial risks to voting rights that computers present and did not allocate regulatory authority sufficient to assure that only accurate and reliable voting machines would be used in federal elections. As 2009 commences, the regulatory gap remains unredressed.

II. The Voting Technology Regulatory Regimes: Pre-HAVA and HAVA

Although the Constitution authorizes Congress to "make or alter" the states' rules concerning the "Times, Places, and Manner" of holding federal elections,[43] Congress has never delegated to any federal agency regulatory power that mandates state compliance with a set of federal minimum standards for voting equipment.[44] Preceding the Help America Vote Act, Congress had impliedly vested in the Federal Election Commission (FEC) some regulatory authority over technologies used in elections, but this was only to generate voluntary standards.

A. PRE-HAVA

In 1975 the National Bureau of Standards, the predecessor agency to the National Institute of Standards and Technology, issued a report concluding that computers could be effectively used as voting machines. But the report noted that its recommendation was conditional. Only if there were "technical improvements of the machines" and "better management of the election process," as well as "formalized guidelines and greater computer expertise" so that election officials could make "informed purchasing decisions," could computers be responsibly integrated into voting.[45] The study specifically noted gaps in information and design between the types of equipment that could be effectively deployed and the market power of officials to stimulate manufacture of the products needed.[46] However, it did not acknowledge the extended gestation that would be required to develop a good computer-based voting system because of the complex software that would need to be written and tested. Nor did the study adequately consider the likelihood or mechanisms by which election officials could receive education in managing the risks of computer-based voting equipment.

More than ten years later and after additional studies, the FEC's Office of Election Administration finally began work to generate federal voting equipment standards. This effort eventually resulted in the first set of FEC voluntary standards that were published in 1990. Beginning with this first standards-setting effort, voting system vendors played a major role. Roy Saltman has noted that, perhaps owing to inadequate funding, the FEC did not utilize independent assessments external to the industry, but instead leaned heavily on the vendors for technical input.[47] This FEC dependence on vendors and its failure to involve, for instance, academic computer scientists, may have been a leading cause of the total omission of strong standards for security, voter, and ballot privacy, usability, documentation, configuration management, and quality assurance and auditing systems.[48] This omission of independent computer scientists may have been the fateful wrong turn that led to over 15 years of computer-based voting technologies that failed to include, for instance, high security and reliability among the core design criteria.

Nearly ten years later, after the obsolescence of the prior standards and the GAO's stern chastisement of the agency for its failure to update standards to stay abreast of technological developments, the FEC returned to the task of drafting voting system standards. Again, the agency omitted most academic and other independent computer scientist expertise. The National Association of State Election Directors (NASED) collaborated with the FEC, eventually producing the two-volume proposed voluntary standards. After a notice and comment period, followed by revisions, the FEC approved the 2002 Voting System Standards.[49]

Under the FEC approach, and preserved by the EAC through its first years,[50] NASED certified the laboratories that conducted voting system testing. The labs were known as ITAs or independent testing authorities. The FEC–NASED testing procedures allowed vendors to contract with an ITA for "qualification" testing.[51] The 2002 standards charged vendors to design and test their voting systems and to document all initial product and system development and internal corporate testing. Once the vendor's own testing supported a conclusion that the voting system satisfied the 2002 FEC voluntary standards, the vendor contracted with ITA Wyle Laboratories, or later SysTest, to conduct the full system testing of hardware and firmware.[52] (The term "firmware" refers to software embedded in a voting system.) The testing procedures required the vendor to submit all documentation of internal testing and test results to the ITA in what came to be known as a Technical Documentation Package, or TDP. The testing regime charged the testing laboratory to review the TDP and conduct system testing consistent with the FEC standards. If deficiencies were identified in testing, the ITA often would provide opportunities for the vendor to correct the problems.

After a voting system's hardware received an ITA recommendation as qualified, the FEC required a software and documentation review by another laboratory that was specifically certified for this work. After the 2002 FEC standards were issued, CIBER Labs and SysTest held this ITA accreditation.[53]

Each testing lab independently reported its testing results and recommendations to both NASED and the vendor in a written report that was branded "proprietary" and thus highly confidential. Even a state's chief election officers and their internal certification processes often faced insurmountable obstacles to accessing the ITA testing reports. NASED maintained a Voting System Committee that was expected to undertake a close review of the ITA reports and recommendations, and to issue a NASED number if the system had qualified as complying with the FEC 2002 standards. As the GAO notably emphasized, though:

> No federal agency has been assigned responsibility for or assumed the role of testing voting equipment against the federal standards. Instead, the National Association of State Election Directors, through its Voting Systems Committee, has assumed responsibility for implementing the federal voting equipment standards by accrediting independent test authorities, which in turn, test equipment against the standards.[54]

Thus, in 2001 the GAO flagged the voting system testing regulatory gap for Congress's remedial consideration. The Help America Vote Act proved to be Congress's response.

B. HAVA'S AUTHORITY FOR FEDERAL VOTING SYSTEM STANDARDS AND TESTING

HAVA articulates mandatory minimum standards for all voting systems used in federal elections from 2006 forward.[55] While the provision of some mandatory statutory standards is a step forward, the standards are predominantly functional rather than technical. With one exception, HAVA left the voting system technical specifications a matter of state discretion. The Act requires, however, that all voting systems that states purchase using HAVA funding or that they deploy in federal elections after January 2006 include the following:

- "Second-chance voting" or "notice voting," meaning the capacity to notify voters of any overvote ballot errors before their ballot is cast, and to provide an opportunity to correct the ballot;
- At least one voting device per precinct that is accessible to disabled voters;
- A manual audit capability;
- Additional language accessibility, as per the Voting Rights Act, section 201;
- Proof of accuracy in the form of an operational error rate that does not exceed the FEC's standard in 2002.[56]

HAVA also required states to define a valid vote for each type of authorized voting equipment.[57]

HAVA responded to the 2000 election issues by assigning to the newly created federal EAC various duties with respect to voting systems, including approval of new voluntary voting system guidelines, accreditation of testing laboratories (with NIST functioning as technical adviser), and certification, decertification, and recertification of voting systems.[58] HAVA initiated explicit federal authority for these crucial activities. The Act also transferred the FEC informational clearinghouse duties to the EAC, including reports regarding voting systems performance.[59]

Neither HAVA nor any other federal Act compels states to deploy only those voting systems that have obtained either an EAC certification or a 2002 FEC-NASED qualification that would presumptively suggest the system satisfies the applicable federal technical standards. Nor does any federal Act require states to test for proof that their voting systems satisfy the HAVA statutory mandates for vote tally accuracy or disability access. Rather, compliance with the federal technical standards for achieving security, reliability, and other objectives remains a matter of discretionary state governmental decision making, with those standards continuing to be typed "voluntary guidelines."[60] HAVA's statutory standards for functional performance of voting systems are mandatory, yet HAVA failed to initiate a federal compliance program or to require states to craft their own. The 2008 performance of voting systems suggests HAVA's mandatory voting system standards were treated as merely hortatory.

Turning to the impact of the voluntary technical standards and the EAC's new certification regime, the EAC's regulatory actions provide some basis for concluding that voting systems certified under its HAVA authority will reach somewhat higher technical standards for reliability, security, and accuracy. The EAC approved the 2005 Voluntary Voting System Guidelines, which became effective in December 2007. With NIST's technical assistance, the EAC adopted a substantially more exacting set of standards and accreditation reviews for Voting System Testing Laboratories, or VSTLs.[61] When NIST first evaluated the former ITAs—the labs that had approved the flawed voting systems widely deployed in 2008 and earlier years—for new certification as VSTLs, it recommended only one as an interim VSTL.[62] During most of 2008, the VSTLs were reviewing voting systems that vendors had submitted for EAC certification pursuant to the 2005 VVSG standards. No voting system has yet been EAC-certified, however. Thus, the 2008 election cycle record does not reflect on the substantive adequacy of the EAC's VVSG and its testing regime.[63]

The problematic voting systems deployed in the 2008 election cycle were permitted under pre-HAVA testing rules, not authorized under the EAC and HAVA testing regime. Depending on the state voting system certification requirements and the state's use of HAVA monies, a state's voting systems deployed in 2008 (1) might have been required to satisfy the FEC–NASED 2002 standards and weak testing regime, as well as state certification requirements; (2) might have been required to satisfy the state's certification requirements and testing only; (3) might have been required to satisfy only the FEC–NASED qualification testing; or (4) might not have been required to satisfy any certification testing whatsoever. Although HAVA mandated that all voting systems purchased by states and local jurisdictions with HAVA funding satisfy the statutory criteria, HAVA did not require that these systems pass any testing certifying that they comply with the statutory criteria before deployment in federal elections.[64]

In sum, while appearing to enunciate mandatory statutory standards for voting systems purchased with HAVA funding, HAVA was pervaded with regulatory gaps and vacuums that undermined its effectiveness in upgrading voting system performance. The first major error lay in disbursing HAVA's substantial voting systems funding before the EAC, its Technical Guidelines Development Committee, and NIST had completed their work to strengthen voting system standards and introduce meaningful, comprehensive certification lab testing. In 2006 and 2007, a series of independent assessments clarified the profoundly deficient lab testing that was performed by ITAs.[65] Acting on NIST's recommendation, the EAC declined to accredit CIBER as an approved interim VSTL.[66] By some estimates, CIBER had conducted the lab testing of voting equipment on which over 65 percent of voters were casting their ballots in 2006.[67]

The California TTBR evaluations of vendor operator manuals and technical reports publicly confirmed the suspicions regarding CIBER's documentation and software evaluations.[68] For instance, the CIBER evaluation of the Diebold GEMS tabulation software summarily concluded in only three short paragraphs that the GEMS software had satisfied scores of complex testing requirements, and did not include any descriptions of required software testing that the lab had conducted. CIBER presented in but one paragraph its platitudinous assessment of the adequacy of over 30 Diebold operational manuals in light of usability, accuracy, and the other FEC standards.[69] The researchers concluded it was not possible to determine whether CIBER had conducted any testing, or which tests it had conducted with what types of results.[70]

A second sequencing problem in HAVA facilitated the error discussed above. Congress specified an overly ambitious but mandatory timetable for purchase and initial launch of the new voting technologies, requiring that the systems be used no later than the first federal election in 2006.[71] HAVA's enactment in late 2002, its specification of a new, more rigorous certification and testing regime to be instituted in relatively short order, and its $2 billion in expected one-time appropriations for new voting technologies apparently invited vendors to engage in strategic behavior. Vendors' optimal strategy for the greatest market share with the fewest regulatory obstacles lay in pushing speedy sales to new HAVA-endowed jurisdictions.[72] HAVA did not explicitly permit the EAC to withhold HAVA funding until a vendor could prove that its system satisfied the stricter performance standards, and the EAC determined that it would not interpret HAVA to require this proof.[73] Ultimately, HAVA's expedited timetable appeared to result in vendors making only slight adjustments to existing voting system product lines. Vendors then rolled out the equipment quickly for HAVA-funded purchases instead of designing, building, and testing higher-assurance voting equipment.

HAVA's goal of improving voting systems was undermined by yet a third legislative mistake: the Act dedicates too little attention to the regulatory, managerial, and technological infrastructure that is needed to support a dramatic technological systems shift and then maintain technological security and reliability. Consistent with its prevailing pro-market faith, the HAVA Congress apparently assumed the market would adequately satisfy the technical needs.[74] It seriously underestimated the risks to voting presented by computerized systems, and the infrastructural staffing, education, and regulatory guidance that would be needed in a computer-based voting world. By indulging the traditional deference to state and local decision making in election administration, Congress inadvertently undermined the capacity of local officials to conduct administratively competent and technically secure elections. HAVA provided lavish financial incentives for moving to technologically advanced voting equipment that generated new risks, but omitted the support that would educate and empower officials to protect voters and the fair administration of elections. The largely invisible risk to computerized elections—a matter beyond any cavil to the computer scientists who have studied the issues—was treated as a matter of marketing and conflicting opinion, rather than scientific judgment and effective public protection for fundamental voting rights. By this educational omission, HAVA exacerbated the conflict between sound science and election officials' discretionary management of election administration.

As the 2008 election cycle drew to a close, neither the federal regulatory apparatus nor most state governments had provided the technical expertise needed for ongoing local support of computer-based elections. HAVA started the ball rolling, but then largely abandoned election officials; the officials were left to obtain technical information from vendors' marketing teams, which invariably promised that the voting systems would perform admirably. Instead of being penalized for fatally ambiguous or erroneous documentation, vendors have in effect been financially rewarded for their documentation failures. Electronic voting equipment has proved so complex and temperamental that even cash-strapped local jurisdictions have had little choice but to contract with the same vendors for additional expensive technical services contracts.

In its effort to show respect to state governments' traditional powers over elections, Congress also failed to supply even interim guidance in effective and secure management of complex computer-based equipment, thus undermining the ability of state regulatory systems to protect election integrity and administrative competency. The elections policymaking and oversight apparatus lacked the requisite technical expertise to provide local officials with procurement and ongoing technical guidance that would ensure election integrity.

Finally, Congress's prevailing faith in the market to produce exemplary election equipment constituted the fourth major regulatory mistake. The voting equipment market's defects in 2002 and continuing into 2009 include substantial market concentration reaching oligopolistic levels; significant barriers to market entry; an artificial "market" composed exclusively of state and local governmental purchasers; and regulatory mandates placing a premium on rapid procurement. Instead of stimulating vendors to design and manufacture outstanding voting systems, the statutory incentives favored vendors who brought their wares to market most rapidly. Trumpeted by glowingly positive marketing campaigns, both the software and hardware were heavily cloaked by stringent proprietary legal clauses that obstructed customers' close evaluations both before and after purchase.[75] A belief in an unregulated market's sufficiency is especially unwarranted where governmental entities are the sole buyers as this factor blocks normal market dynamics. Given the critical social and political importance of honest elections, and the indisputably defective market dynamics, the congressional gamble on trusting the market was unwarranted.

III. The 2008 Record of Statewide Voter-Registration Databases

All states but one (North Dakota) require voters to be registered in advance of voting. In the United States, voter registration systems are used to regulate access to voting. The government seeks to ensure that only those persons legally entitled to vote in a given jurisdiction are permitted to do so, and that each person votes only once in a given election.[76] Because voter registration lists determine who is allowed to vote, these lists constitute one point for potential wholesale disruption of elections for strategic gain.[77]

In reviewing Florida's record in the 2000 presidential election as well as some other states' performance in voter registration record maintenance,[78] HAVA's sponsors recognized that states had neglected to provide ongoing supervision and protection of voter registration lists.[79] Generally maintained at the county level, some voter lists were replete with errors that could cause voter disenfranchisement. The hypothesized causes ranged from local officials' inadvertent mismanagement to deliberate mischief for partisan gain. The HAVA Congress perceived the answer to these risks to lie in a statewide voter-registration database that the state's chief election officer would manage.

HAVA's core mandate provides for each state to implement "a single, uniform, official, centralized, interactive computerized statewide voter-registration list defined, maintained, and administered at the state level that contains the name and registration information"[80] of the legally registered voters in the state. Additionally, the list must assign a "unique identifier"[81] to each of these legally registered voters. The Act elaborates a variety of additional design and operational requirements for the statewide database, including a requirement that its data be consistent with the Department of Motor Vehicles drivers' license database and with several other lists. It also specifies a range of technical managerial activities.[82]

Creating a statewide voter-registration database is a complex technical task. It requires state officials to combine many county databases, which have been separately developed and maintained, into one unified database. Further, a statewide database must include a unified update process. This task is exceedingly error prone for states with more than a handful of counties because the different databases are often built with different software, in most cases proprietary, or no software at all in cases where a jurisdiction still uses paper registration records. A large number of small but vital incompatibilities inevitably appear when data from two separate sources have to be unified.

Voters' names alone provide many sources of error. One source might record a single field for the name of the voter as opposed to two fields for the first and last names, or middle initials vs. full middle names, or formal names ("James") vs. informal ("Jim"), or married vs. single names. There may be orthographic differences, where one data source includes Spanish accents, German umlauts, and other diacritics but another drops them. The problem becomes even more complex and fraught with error when states "clean" the unified database by attempting to purge it of duplicates, felons, or deceased persons. One such difference in data conventions almost resulted in an apparently ethnically biased registration database purge in Florida in 2004, because the registration data recognized "Hispanic" as a racial category, whereas a list of felons being purged from it did not.[83] The problem was recognized and the purge was canceled.

In mandating statewide voter-registration databases, Congress appears not to have recognized the demandingly high level of technical database design expertise and costly maintenance that would be imposed on states. Nor did it comprehend the risks the statutory requirement would present to registration data that constitutes the gateway to electoral participation. For instance, determining whether two data entries that have been recorded independently under different procedures and conventions refer to the same person is a notoriously error-prone task. Registration-database purging based on matching of names and other nonunique data have been involved in the wrongful disenfranchisement of thousands of voters. The most notorious example remains the registration purges the Florida Division of Elections ordered in 2000.[84]

As these database-updating problems have become more recognized, some states have begun to rely more on unique identifiers, such as driver's license numbers and social security numbers, rather than on exact name matching before deleting voters. Florida again provides a key example. In 2007, the Florida State Conference of the NAACP filed suit in federal court to strike down a provision of Florida's registration law that required the state to match the prospective voter's name and driver's license number or social security number on a voter registration application with the same information in DMV and Social Security databases.[85] The NAACP argued that the name-matching requirement would produce many erroneous matching failures because of the general problems with name matching. Further, the NAACP contended that additional erroneous match failures would result from innocent clerical mistakes made by voters in writing down the lengthy HAVA-required unique identifier numbers on the registration application or from numerous transcription errors made by state clerks in entering the data from those applications. The evidence established that a high rate of county officials' transcription errors occurred that were no fault of the applicant. The case was largely resolved by Florida's statutory reforms to correct some of the problems claimed in the suit.[86]

While electronic voting systems have now received considerable scrutiny by independent experts, the same cannot (yet) be said of statewide registration databases. As required by HAVA, states have been consolidating local registration databases into statewide registration databases along with procedures for their administration, but the indicators are that many states have undertaken these tasks with little or no consultation from qualified independent technical experts. A large number of accuracy, security, privacy, and data maintenance issues related to the initial construction of those databases and to their maintenance have been published in the popular press.[87] In many cases, state election agencies lack the staff expertise for handling them with the care requisite to protecting fundamental voting rights. Some state election agencies may also lack the technical expertise for identifying the appropriate set of advanced technical skills needed in advisers for such a demanding database project, but no detailed federal guidance has issued from the EAC.

All of the problems with registration databases that have arisen so far were eminently predictable given the technical demands HAVA specified, the lack of consistent software among the databases that must interrelate for consistent updating, and the lack of consistent data held in the databases. By contrast with the proprietary voting systems, state election agencies could resolve most if not all of the statewide database technical problems with the appropriate technical expertise. Technical firms' overstatement of their qualifications and desire for ongoing service contracts can keep state agencies from procuring appropriately designed and updated statewide databases, instead leaving them with a patchwork of partial solutions and a steady stream of expensive contracts. Hence, independent experts who do not seek an ongoing services contract (similar to those convened for the TTBR study) might be a wise initial step. Of particular concern and presenting yet new technical demands is the relatively new idea of online voter registration, as permitted in Arizona and (soon) California. Another key concern and omission: thus far, no comprehensive independent technical studies have been convened and published that determine the statewide databases' security, accuracy, reliability, and compliance with federal voting rights laws. Deficiencies in any of these areas may seriously affect thousands of voters' franchise rights.

As with voting sÿstems, Congress's application of computer technology to voter registration reflected an idealistic vision of the opportunities the database technology offered, one that does not recognize or provide sufficient protection from the attendant risks. Unlike its treatment of voting systems, HAVA unfortunately omits explicit federal regulatory authority for minimum voluntary or mandatory technical standards by which the functional statutory objectives will be achieved. Instead, HAVA directs that the "appropriate State or local official shall provide adequate technological security measures to prevent the unauthorized access to the computerized list. . . ."[88] In mandating a move to statewide voter-registration databases, Congress again sets many state officials adrift, making them vulnerable to marketing ploys because they lacked the high level of technical expertise necessary to protect the voters' franchise rights and ensure the registration systems' basic functionality.[89]

Some advisory federal efforts have been initiated to raise state agencies' appreciation of the security risks and technical challenges in managing statewide registration databases. In 2005, NIST convened a workshop titled "Threats to Voting Systems," which included discussion of threats embedded in statewide voter-registration systems.[90] The EAC also cosponsored workshops for state election officials, including with the National Academies,[91] on performance challenges underlying the required statewide databases. These efforts began only after the technological idealism had faded somewhat and the challenging reality that HAVA had imposed on state officials became palpable.

Some published papers have shown that the technical challenges are not merely hypothetical.[92] In one major report, the authors noted the lack of agreement even on whether HAVA authorizes the EAC to articulate guidance or national consensus standards that might be considered best practices for the statewide voter databases.[93] In their conclusion, they argue that three elements are missing from any definition of a successful implementation of a statewide voter-registration system under HAVA:

1. A set of national consensus standards for voter registration systems.
2. A set of consensus performance measures to determine the extent to which the systems exhibit the desirable characteristics.
3. Means of obtaining the necessary information for those metrics.

In 2007, the EAC commissioned a study of official voter information websites, which often include an online connection (interface) to the statewide voter-registration database. The study report was submitted in late 2008[94] with recommendations of a number of best practices that seek to protect the data and reliability of the voter information website. The study's researchers reviewed more than seventy websites to produce the assessments. In addition to finding some effective sites, the lead researcher commented that he was "surprised at the amount of information about registered voters some officials were putting online."[95] Despite its classification as "public" information, he viewed some sites as creating the risk of identity theft.[96]

The study included a number of recommendations whose predicates reveal that many state agencies' statewide databases fail to satisfy basic precepts by which data security and privacy are achieved. For instance, the researchers advised that such websites "should be carefully constructed to avoid jeopardizing voters' privacy or the integrity and security of the records."[97] It also cautioned officials to be sure that any interface to the registration database on a website is, of course, to a copy of the database rather than the live original, so that there is no possibility of accidental or malicious modification of registration data through the Internet.[98] The study recommended that state governments consider outsourcing the development of these websites, use commercial or open-source tools and software, plan to accommodate spikes in demand, and promote the sites' use. The researchers urged that HAVA section 508 requirements be viewed as stating the minimum standards for accessibility and that administrators control and limit the amount of data exposed.

Some states have experienced significant continuing problems with the HAVA-mandated registration databases. In Wisconsin, for instance, 11 percent of voters cannot currently be matched against other state lists. Its Government Accountability Board notes that this 11 percent reduces by half the mismatches found in August 2008, when 22 percent of voters' data entries were inconsistent as between databases.[99] The database mismatching spawned significant litigation in Ohio and Wisconsin during the 2008 general election, with some suggesting that mismatches indicated voter fraud.[100] Unfortunately, the paucity of technological understanding regarding the design, reliability, security, and accuracy of these registration databases may lead to an unwarranted public belief that fraud has occurred.

As the 2008 election cycle concluded, abundant indicators of serious technical deficiencies in the statewide voter-registration databases had arisen across the nation. No federal or independent study, however, appears to have been planned to assess the statewide registration databases' basic functionality or compliance with HAVA, as part of the EAC's research work or federal legislative agenda. The technical features and deficiencies of these mission-critical registration databases remain shrouded in secrecy. The federal agencies do not consider the databases within their core regulatory or advisory mandates; many state election agencies and their leadership are apparently ignorant of the grave risks the substandard database designs pose and are reluctant to provide public transparency; and the technical issues can be daunting to policymakers at every governmental level. But this set of regulatory circumstances means there is no federal or other public accountability for the highly vulnerable public gateways into the electoral system and the concomitant rights of popular sovereignty.[101] Further, neither voter registration database performance metrics nor independent compliance reviews are currently planned to fulfill duties of election administrative transparency and accountability to the public.[102]

The federal experience with the statewide voter-registration databases appears to track that of voting technologies. With both technologies, their inception has been marked by enthusiasm and idealism about the technological prospects, followed by serious and unexpected deficiencies in technical system performance or surprise from the fiscal issues that arise from the technology, followed by a more mature recognition of the prospects, risks, and costs attending the technology. Importantly, mature governmental judgment regarding voting systems has involved advice and reports from independent technical experts such as those from major academic institutions. As occurred with voting systems, critical evaluations by teams led by highly qualified academic technical experts may be needed in order to obtain "top to bottom" evaluations of the databases' technical sufficiency.[103] These independent experts' involvement may be necessitated to diagnose, document, and recommend appropriate remedial technical steps and standards for safeguarding essential voting rights and achieving electoral administrative success untainted by financial interests in obtaining long-term consulting contracts.

IV. Conclusion

To a great extent and with the best of intentions, HAVA generated a vast national experiment with one of the most fundamental and vulnerable of our civil rights. While technical understanding may be improving at both the federal and state levels, the sophisticated technical systems HAVA embraced pose threats to the franchise. Before embarking on any new technological experiments in elections, the nation must revisit the elections IT regulatory structure. Computer-based election equipment should not be deployed bereft of a policy apparatus that is structured and staffed so that it can remain fully informed of the dynamically developing technological knowledge relevant to ensuring election accuracy, security, and other core objectives while also preserving voter access.

Notes

1. U.S. Commission on Civil Rights, Voting Irregularities in Florida During the 2000 Presidential Election (June 2001), *available at* http://www.usccr.gov/pubs/vote2000/report/main.htm; Bush v. Gore, 531 U.S. 98 (2000).

2. Help America Vote Act of 2002, 42 U.S.C. §§ 15301-15545 (2002). Curiously, in enacting HAVA, Congress supplied none of the common sources of legislative history. The omission of Committee Reports is a particular loss. The omissions leave legal scholars and regulatory entities to rely on contemporaneous public discussions, interviews with congressional Committee staff, and reports of other federal entities that studied the 2000 election. For instance, see Leonard M. Shambon, *Implementing the Help America Vote Act*, 3 Election L.J. 424 (2004), whose author was Counsel to Rep. Steny Hoyer of Maryland. Hoyer was the ranking (minority) member of the House Administration Committee, in whose jurisdiction federal election law is reposed, and was a primary coauthor of the bipartisan HAVA bill. *See also* Commission on Civil Rights, *supra* note 1.

3. 42 U.S.C. § 15481; *see infra* part II.B.

4. HAVA required technology purchased with Title I and Title III funds to be launched no later than the first federal election of 2006. *See* 42 U.S.C. §§ 15302(a)(3), 15481(d).

5. 42 U.S.C §§ 15321-15330.

6. *See* Shambon, *supra* note 2, at text accompanying note 32 ("HAVA has the effect of moving from an environment of loose state and limited federal oversight to an environment of strong state control").

7. Interview with former House Administration Committee senior staff member Patrick Sweeney, October 2005.

8. HAVA created the U.S. Election Assistance Commission (EAC), *supra* note 5. The only mandatory regulatory authority Congress vested in the EAC was that HAVA transferred from the Federal Election Commission (FEC) pursuant to the National Voter Registration Act. *See* 42 U.S.C. §§ 15531, 15532.

9. *See, e.g.*, 42 U.S.C. §§ 15381-15387, 15501. As the EAC website states, "One of EAC's top priorities is providing assistance to election officials. EAC has issued guidance, advisories and best practices to help them comply with HAVA and make other election administration improvements and enhancements." http://www.eac.gov/election.

10. See http://www.votersunite.org for an extensive inventory of press reports of voting technology malfunctions and the vendors' explanations, dating back to 2004. The site permits searching by year, vendor, or type of issue. Some examples of attributing technology malfunctions to election officials and other operators include Sequoia Voting Systems' blaming human error in Washington, D.C., *see* Nikita Stewart, *Voting Database Is Fine, Firm Says; User Error Cited as Possibility in D.C. Vote Foul-Up*, Wash. Post, Sept. 12, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/story/2008/09/12/ST2008091200149.html; and Premier/Diebold's blaming election officials for errors in Florida's Hillsborough

County, *see Governor Asked to Intervene in Hillsborough County Elections*, Nov. 6, 2008, http://www.votersunite.org/article.asp?id=8184.

11. *See, e.g.*, the California Secretary of State's Top to Bottom Review of Voting Systems conducted by the University of California, summer 2007, http://www.sos.ca.gov/elections/elections_vsr.htm.

12. EAC, STATE GOVERNMENTS' USE OF HELP AMERICA VOTE ACT FUNDS table 2.1 (July 2008), *available at* http://www.eac.gov/election/HAVA%20Funds/docs/2007-report-on-hava-spending-by-states/attachment_download/file.

13. *See* Stephen Ansolabehere & Charles Stewart III, AMERICA VOTES!, at 241.

14. *See, e.g.*, NATIONAL COMMISSION ON FEDERAL ELECTION REFORM, TO ASSURE PRIDE AND CONFIDENCE IN THE ELECTORAL PROCESS (Aug. 2001) ("Ford/Carter" Commission), *available at* http://www.reformelections.org/data/reports/99_full_report.pdf.

15. Bush v. Gore, 531 U.S. 98, 103 (2000).

16. In an "overvoted" race, a ballot has been marked with more choices than the race permits, such as selecting two candidates for one legislative seat. An overvoted race will not record either selection but voids the ballot for that race. Some faulty ballot designs are blamed for high overvote rates. An "undervoted" race results in no recorded or readable vote in the race. *See generally* LAWRENCE NORDEN, DAVID KIMBALL, WHITNEY QUESENBERY & MARGARET CHEN, BETTER BALLOTS (2008), *available at* http://brennan.3cdn.net/d6bd3c56be0d0cc861_hlm6i92vl.pdf (discussing ballot design principles that augment voter accuracy).

17. Before HAVA, in the absence of explicit statutory authority, the FEC had attempted to redress the regulatory vacuum by developing and issuing its recommendations of standards for voting systems performance and lab testing. The National Association of State Election Directors (NASED) created and administered a program to qualify voting systems as being in compliance with the FEC standards. Within this certification system, NASED used the term "qualified," reserving the term "certified" for a state's formal decision that a voting system was acceptable according to its own standards, which in many cases required satisfaction of the FEC standards. *See infra* part II.A.

18. HAVA's primary mechanism for infrastructural support was the creation of the U.S. Election Assistance Commission and its related advisory boards detailed in the text. *See* 42 U.S.C. §§ 15321–15330.

19. 42 U.S.C. § 15302; *see infra* part II.B. Dan Tokaji has written extensively about the discriminatory racial and ethnic effects of voting technology choices. *See, e.g.*, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1741–67 *passim* (2005).

20. *See* Ansolabehere & Stewart, *supra* note 13, at 252–53. Other accessible technologies exist and arguably have a better or competitive accessibility and performance record as compared with the major technologies. The Vote-PAD, for instance, claims to be an "inexpensive, non-electronic, voter-assist device that helps people with a broad range of visual or dexterity impairments to vote independently." http://www.vote-pad.us/.

21. Although some scanning systems are "optical" scanners that read and record the voting data, and others are "digital" scanners that digitally photograph each ballot as well as record the voting data, for purposes of this chapter "optical scanning" designates both technologies.

[22] E.g., ES&S presents its touch screen: "The patented iVotronic™ Touch Screen Voting System is the premier voting solution for jurisdictions who prefer paperless voting. Available with a 15" full-color display, the iVotronic is wireless, multilingual, and ADA-compliant. Voters securely cast their vote for each race and/or ballot proposition simply through the touch of the screen. Its Audio Ballot feature easily assists those voters who are visually impaired." http://www.essvote.com/HTML/products/ivotronic.html.

[23] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin & Dan S. Wallach, Analysis of an Electronic Voting System, Johns Hopkins University Information Security Institute Technical Report TR-2003-19 (July 23, 2003), *available at* http://avirubin.com/vote.pdf.

[24] "DOS" attacks or denial of service and operability. Voting machines failing to boot up on Election Day could be a reliability issue or an example of an attack that is disguised to appear as simply a malfunction. *See generally* Matt Bishop, Computer Security: Art and Science (2002).

[25] Given the high financial value of control over government policy, and the impact of government over private sector assets and economic opportunities, voting would seem to be an inherently vulnerable activity. "Voting systems demand accuracy and security, and if they fail to meet these properties, so will the election. Developing mission-critical systems requires the application of high-assurance techniques. These systems must incorporate features not normally included in other systems (such as redundancy, validation mechanisms, and fail-safe controls) so they require a rigorous development process." A. Yasinsac & M. Bishop, *The Dynamics of Counting and Recounting Votes*, 6 IEEE Symp. Sec. & Privacy 22, 25 (2008). *See generally* Matt Bishop, An Introduction to Computer Security 1.5, 1.6.2, and ch. 18 (2005).

[26] *See, e.g.*, the studies listed in Matt Bishop, Mark Graff, Candice Hoke, David Jefferson & Sean Peisert, Resolving the Unexpected in Elections: Election Officials' Options, Appendix 2: Partial List of Voting Systems Studies at 22–27, *available at* http://www.electionexcellence.org/ (reviewing forensics for electronic voting systems).

[27] The TTBR reports are published at http://www.sos.ca.gov/elections/elections_vsr.htm. A two-page summary can be found at http://www.electionexcellence.org. Matt Bishop, one of the principal investigators, noted that he and the other TTBR researchers "did not focus on the criteria that the machines *should* meet. The criteria were specified in the project's Statement of Work. We instead focused on how well those criteria were implemented, both by the design and construction of the system." E-mail message from Bishop to coauthors, January 8, 2009. The time-bound study also noted a number of means by which voting results accuracy could be subverted.

[28] The Ohio Secretary of State's EVEREST reports reviewed some of the same voting systems as in California except the ES&S systems were included and the Sequoia systems were not. http://www.sos.state.oh.us/SOS/elections/voterInformation/equipment/VotingSystemReviewFindings.aspx.

[29] *See* Bishop et al., *supra* note 26, for an inventory of the most significant voting systems research assessing deployed systems (with links).

[30] *See supra* note 25.

[31] The former president of the California Association of County Election Officials (CACEO), Steve Weir, responded to the TTBR: "It was a test that was conducted in a laboratory

without any of the protections that we have on our systems. And in theory—and only in theory—were these systems vulnerable. . . . But there's no proof that it has been done." http://www.pbs.org/newshour/bb/politics/jan-june08/ballot_01-16.html.

32. Ohio's election officials responded in a measured tone, suggesting that discussions on "remediation" ensue. http://www.acluohio.org/issues/votingrights/OAEOStatementInResponseToEVEREST2008_0122.pdf.

33. The Verified Voting Foundation, http://www.verifiedvoting.org, and Voters Unite, http://www.votersunite.org, offer useful research resources on voting technology issues.

34. *See, e.g.*, the report coauthored by three major national research and advocacy organizations: *Is America Ready to Vote? available at* http://www.brennancenter.org/content/resource/is_america_ready_to_vote/ (partnering Common Cause, Verified Voting Foundation, and the Brennan Center for Justice).

35. All voting equipment technical issues recounted in text accompanying notes 34–39 can be found at http://www.votersunite.org, in the "Election Problems" inventory that is searchable by state, date, or type of problem.

36. In 2008, Super Tuesday occurred on February 5 as 24 states held primaries or caucuses. The day's tallies produced 52 percent of pledged Democratic Party delegates and just over 40 percent of the total Republican Party delegates. *See* Dan Balz, *Feb. 5 Primaries to Pose a Super Test of Strategy,* WASH. POST, Jan. 15, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/01/14/AR2008011402926_pf.html.

37. ANDREW W. APPEL, MAIA GINSBURG, HARRI HURSTI, BRIAN W. KERNIGHAN, CHRISTOPHER D. RICHARDS & GANG TAN, INSECURITIES AND INACCURACIES OF THE SEQUOIA AVC ADVANTAGE 9.00H DRE VOTING MACHINE, http://citp.princeton.edu/voting/advantage/.

38. Summarized by VotersUnite! at http://www.votersunite.org/electionproblems.asp?offset=280&sort=date&selectstate=ALL&selectvendor=&selectproblemtype=ALL (emphasis added).

39. *See, e.g.*, VotersUnite! testimony for EAC public hearing, Dec. 3, 2008, *available at* http://www.votersunite.org/info/EACTestimony12_8_08.pdf (written testimony urging tracking).

40. JOE HALL, PRELIMINARY ANALYSIS OF OVL VOTING EQUIPMENT REPORTS, http://www.josephhall.org/nqb2/index.php/2008/11/12/p1105.

41. The California TTBR report on the accessibility of three major voting systems with regard to specific physical impediments documented pervasive non-usability of the supposedly accessible voting devices. *See Noel Runyan & Jim Tobias, Accessibility Review Report for California Top-to-Bottom Voting Systems Review, available at* http://www.sos.ca.gov/elections/elections_vsr.htm.

42. *Id.*

43. U.S. CONST. art. I, § 4.

44. Indeed, a GAO report found that Congress had never explicitly authorized a federal agency to develop voting system standards. *See* U.S. GENERAL ACCOUNTING OFFICE, ELECTIONS: STATUS AND USE OF FEDERAL VOTING EQUIPMENT STANDARDS, GAO-02-52, at 4 (Oct. 2001), *available at* http://74.125.95.132/search?q=cache:5P2zJZMp5OkJ:www.gao.gov/new.items/d0252.pdf+%22gao-02-52%22&hl=en&ct=clnk&cd=1&gl=us.

45. Eddan Katz and Rebecca Bolin, *Electronic Voting Machines and the Standards-Setting Process*, 8 J. INTERNET L. 4 (2004), referring to an NBS report authored by Roy Saltman, EFFECTIVE USE OF COMPUTING TECHNOLOGY IN VOTE TALLYING (1975).

46. *Id.*

47. ROY G. SALTMAN, THE HISTORY AND POLITICS OF VOTING TECHNOLOGY: IN QUEST OF INTEGRITY AND PUBLIC CONFIDENCE (2006).

48. *See* GENERAL ACCOUNTING OFFICE, *supra* note 44, at 11.

49. http://www.eac.gov/program-areas/voting-systems/voluntary-voting-guidelines/2002-voting-system-standards.

50. 42 U.S.C. § 15362(e); for further discussion, see *infra* note 58.

51. The FEC–NASED regime contemplated three distinct types of technical testing:

- *Qualification* testing is the process by which a [*sic*] voting equipment is shown to comply with the requirements of its own design specification and with the requirements of FEC standards.
- *Certification* testing, generally conducted by individual states, determines how well voting equipment conform to individual state laws and requirements.
- *Acceptance* testing is generally performed by the local jurisdictions procuring voting equipment and demonstrates that the equipment, as delivered and installed, satisfies all the jurisdiction's functional and performance requirements.

GENERAL ACCOUNTING OFFICE, *supra* note 44, at 8.

52. *See id.*; SALTMAN, *supra* note 47, at 180.

53. *See* GENERAL ACCOUNTING OFFICE, *supra* note 44, at 8–10.

54. *See id.* at 5.

55. 42 U.S.C. § 15481(a).

56. *Id.*

57. 42 U.S.C. § 15481(a)(6).

58. Under HAVA, the National Institute of Standards and Technology (NIST) is charged with assisting the EAC in its testing lab certification program through the NIST National Voluntary Laboratory Accreditation Program (NVLAP). NIST recommends laboratory accreditation but the EAC makes the final decision to accredit laboratories.

59. 42 U.S.C. § 15222(1), incorporating by reference the duties of 42 U.S.C. §§ 15361 *et seq.* Whether the EAC holds clearinghouse duties to gather and post information regarding the performance of voting systems it did not certify under its new federal testing regime and VVGS standards has been a matter of continuing controversy. At a hearing on Dec. 8, 2008, the EAC heard oral testimony and received written statements regarding its clearinghouse powers and duty regarding these systems. *See* http://www.eac.gov. This chapter's coauthors have concluded that HAVA expressly confers EAC authority, and arguably a statutory duty, to provide voting systems informational (clearinghouse) reporting on voting systems that predate the EAC's certification system. In 42 U.S.C. § 15362(e), HAVA provides that the 2002 FEC standards "shall be deemed to have been adopted by the Commission as of the date" HAVA is enacted. Hence, the FEC standards are now EAC standards, and the clearinghouse reporting duties encompass pre-EAC and post-EAC voting systems.

60. The best example is the EAC's Voluntary Voting System Guidelines. The EAC has documented that all but 20 states required voting systems approved for their state to participate in some form of EAC testing or certification. *See* State Requirements and the Federal Voting System Testing and Certification Program, *available at* http://www.eac.gov/program-areas/voting-systems/.

61. The EAC approved the Voluntary Voting System Guidelines (VVSG) in December 2005. It announced that the VVSG would be effective for all voting systems submitted for certification testing after December 2007. *See* http://www.eac.gov/program-areas/voting-systems/voting-system-certification/2005-vvsg. In July 2006, EAC adopted a phased implementation of its new Voting System Testing and Certification Program. The two phases consist of (1) the pre-election or "interim phase," and (2) the full testing and certification program. The interim phase began in July 2006 and covered only modifications to existing voting systems. On December 7, 2006, EAC Commissioners voted to approve adoption of the full program with implementation beginning in January 2007. As this chapter went to press, the EAC had not yet certified any voting systems under the more rigorous testing program.

62. SysTest was the only ITA that was initially certified as a VSTL, but the EAC revoked its certification after NIST documented that the lab had not been conducting the required tests. *See* http://www.eac.gov/News/eac-announces-intention-to-suspend-systest-labs/base_view.

63. The EAC has sustained criticism for not completing the certification of newer, and presumably much-improved, voting systems in time for purchase and deployment for the 2008 general election. This chapter's coauthors, however, applaud the EAC's refusal to rush voting systems through a less rigorous testing and evaluation process. Given the vital importance of protecting voting rights and the established record of harms caused by flaws in supposedly HAVA-compliant voting systems that were hurried to market with insufficient testing, it is incumbent on public officials to ensure that voting systems meet at least minimum technical standards for performance.

64. The GAO acknowledged the problem in a report; *see* Federal Program for Certifying Voting Systems Needs to Be Further Defined, Fully Implemented, and Expanded, GAO-08-814, Sept. 16, 2008.

65. *See supra* note 29.

66. *See* Press Release, EAC, EAC Accredits Voting System Test Labs, *available at* http://votetrustusa.org/index.php?option=com_content&task=view&id=2278&Itemid=26. In 2008, however, NIST recommended CIBER for EAC accreditation. http://www.eac.gov/voting systems/test-lab-accreditation/laboratories-recommended-for-accreditation-by-nist.

The *New York Times* broke the story concerning CIBER's testing failures. Christopher Drew, *U.S. Bars Lab from Testing Electronic Voting*, Jan. 4, 2007, *available at* http://www.nytimes.com/2007/01/04/washington/04voting.html?_r=1.

67. Joe Hall's estimate is reported in an op-ed piece by Michael Richardson, *Banned Test Lab Certified Electronic Voting Machines Used by 68.5% of Nation's Registered Voters in 2006 Elections*, http://www.opednews.com/articles/opedne_michael__070113_banned__test_lab_cer.htm.

68. The TTBR documentation reviews are published at http://www.sos.ca.gov/elections/elections_vsr.htm. *See* CANDICE HOKE & DAVE KETTYLE, DOCUMENTATION ASSESSMENT OF THE DIEBOLD VOTING SYSTEM, *available at* http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold_doc_final.pdf; JOSEPH LORENZO HALL & LAURA QUILTER, THE DOCUMENTATION REVIEW OF THE HART INTERCIVIC SYSTEM 6.2.1 VOTING SYSTEM, *available at* http://www.sos.ca.gov/elections/voting_systems/ttbr/hart_doc_final.pdf; AARON J. BURSTEIN, NATHAN S. GOOD & DEIRDRE K. MULLIGAN, REVIEW OF THE DOCUMENTATION OF THE SEQUOIA VOTING SYSTEM, *available at* http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia_doc_final.pdf.

69. One coauthor of this chapter, Candice Hoke, was a research team leader and coauthor of the TTBR Diebold Documentation Assessment. She recalls the surprisingly superficial, platitudinous summations concerning the quality of the vendor's software and documentation. The TTBR assessment noted that the CIBER report provided no basis for concluding that the required testing had been conducted or that the voting system had been shown to meet the 2002 FEC standards. See HOKE & KETTYLE, *supra* note 68, at 2–3 (Executive Summary) and part 4.1 (reviewing adequacy of testing lab reports).

70. *Id.*

71. 42 U.S.C. § 15481(d).

72. *See* Thomas P. Ryan & Candice Hoke, *GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standards* 6–7, http://www.usenix.org/events/evt07/tech/ (published as part of the 2007 Electronic Voting Workshop proceedings).

73. *See* EAC Advisory 2005-004: How to Determine if a Voting System Is Compliant with Section 301(a)—A Gap Analysis Between 2002 Voting System Standards and the Requirements of Section 301(a) (July 20, 2005), *available at* http://www.eac.gov/election/docs/eac-20advisory-2005-004301a.pdf/attachment_download/file.

74. HAVA's primary mechanism for infrastructural support was the creation of the U.S. Election Assistance Commission and its related advisory boards detailed in the text. *See* 42 U.S.C. §§ 15321–15330.

75. Joseph L. Hall, *Contractual Barriers to Transparency in Electronic Voting* 4.2–4.4, http://www.usenix.org/events/evt07/tech/ (published as part of the 2007 Electronic Voting Workshop proceedings).

76. JUSTIN LEVITT, WENDY R. WEISER & ANA MUÑOZ, MAKING THE LIST: DATABASE MATCHING AND VERIFICATION PROCESSES FOR VOTER REGISTRATION 23 (Mar. 2006), *available at* http://brennan.3cdn.net/96ee05284dfb6a6d5d_j4m6b1cjs.pdf.

Many factors can affect the accuracy of statewide voter-registration databases. The Association for Computing Machinery (ACM), U.S. Public Policy Committee, produced an important report recommending steps to safeguard the databases. Written for a layperson (not requiring technical training in computer science or engineering), the report includes chapters on security, privacy, accuracy, reliability, and usability. *See* STATEWIDE DATABASES OF REGISTERED VOTERS: STUDY OF ACCURACY, PRIVACY, USABILITY, SECURITY, AND RELIABILITY ISSUES (2006), *available at* http://usacm.acm.org/usacm/VRD/.

77. STATEWIDE DATABASES OF REGISTERED VOTERS, *supra* note 76, at 39–40, 46–49.

78. The U.S. Commission on Civil Rights focused *inter alia* on voter registration issues. *See* COMMISSION ON CIVIL RIGHTS, *supra* note 1, ch. 5, "The Reality of List Maintenance."

79. The Caltech-MIT Voting Technology Project estimated that as many as three million votes were lost in the disputed 2000 presidential election because of problems with the voter registration process. R. Michael Alvarez, Stephen Ansolabehere & Catherine H. Wilson, *Election Day Voter Registration in the United States: How One-Step Voting Can Change the Composition of the American Electorate* 4 (Caltech-MIT Voting Technology Project, Working Paper No. 5, June 1, 2002), *available at* http://vote.caltech.edu/drupal/node/16.

80. 42 U.S.C. § 15483(a).

81. *Id.*

82. 42 U.S.C. § 15483(a)(2).

83. Ted Selker & Alexandre Buer, Voter Removal from Registration List Based on Name Matching Is Unreliable, Voting Technology Project, MIT Media Laboratory, *available at* http://www.vote.caltech.edu/reports/purging-vrdb.pdf.

84. *See* Commission on Civil Rights, supra note 1.

85. The record of the case can be found at http://www.brennancenter.org/content/resource/florida_naacp_v_browning and at http://moritzlaw.osu.edu/electionlaw/litigation/FloridaNAACPv.Browning.php.

86. The Eleventh Circuit declined to hold that federal law preempted the Florida statute, and remanded the case, Florida State Conference of N.A.A.C.P. v. Browning, 522 F.3d 1153 (11th Cir 2008), eventually leading to legislative reforms.

87. *See, e.g.,* Posting of Reginald Fields to Openers: The Plain Dealer Politics Blog, *Jennifer Brunner Cancels Cross-Checking of Ohio's New Voters,* http://blog.cleveland.com/openers/2008/10/brunner_says_voter_registratio.html (Oct. 30, 2008, 12:13 EST); Myung Oak Kim, *New Voter Database Price at $13 Million; Two Years Late, SCORE Will Be Tested April 21, Rocky Mountain News,* Apr. 11, 2008, *available at* http://www.rockymountainnews.com/news/2008/apr/11/new-voter-database-price-at-13-million/.

88. 42 U.S.C. § 15483(a)(3), entitled "Technological Security of Computerized List."

89. For instance, the Pew Center on the States found that 20 states planned to construct their systems in house. *See Assorted Rolls: Statewide Voter Registration Databases Under HAVA* (June 2005), *available at* http://www.electionline.org.

90. R. Michael Alvarez, Potential Threats to Statewide Voter Registration Systems, Caltech/MIT Voting Technology Project, Oct. 6, 2005, *available at* http://www.vote.caltech.edu/media/documents/wps/vtp_wp40.pdf.

91. 5th Meeting of the State Voter Registration Databases, sponsored by the National Academies, Dec. 4, 2008, http://www8.nationalacademies.org/cp/meetingview.aspx?MeetingID=3022. The posted program notes that the second day's presentations and discussions were closed to the public.

The National Academies assisted the EAC in providing some general background guidance for state officials in a 2005 report, *Voluntary Guidance on Implementation of Statewide Voter Registration Lists,* available at http://www.eac.gov/News/meetings/ploneexfile.2006-04-24.4700034238/?searchterm=National%20Academies. Unfortunately, the document lacks important technical specifications for the complex databases that would be required as well as explanations of what types of technical credentials would be necessitated to achieve the HAVA-imposed tasks. For instance, the Guidance directs: "Election officials must also create clear policies and protocols to make statewide voter registration lists secure. The protocols must identify appropriate classes of authorized users. . . ." *Id.* at 17. At a minimum, the document should have advised state officials that they should retain a qualified database security expert to advise on database design for achieving high security and reliability.

92. *See also* LEVITT, WEISER & MUÑOZ, *supra* note 76.

93. ERIC A. FISCHER & KEVIN J. COLEMAN, VOTER REGISTRATION SYSTEMS (2006), *available at* http://www.american.edu/ia/cdem/hava/papers/Fischer_Coleman-Voter_Registration_Systems-AU.pdf.

94. *See* William Jackson, *Voter Sites Face Privacy Risk: Commission Report Recommends Ways to Secure Public but Sensitive Data on Web*, GOV'T COMPUTER NEWS, Dec. 15, 2008, *available at* http://www.gcn.com/print/27_29/47730-1.html?topic=data_management. The EAC posted the study; *see* U.S. ELECTION ASSISTANCE COMMISSION, VOTER INFORMATION WEBSITES STUDY, http://www.eac.gov/program-areas/research-resources-and-reports/completed-research-and-reports/program-areas/research-resources-and-reports/2008_nov_voter_info_website_study/attachment_download/.

95. William Jackson, *Voter Sites Face Privacy Risk*, http://mobile.gcn.com/articles/27_29/47730-1.html.

96. ELECTION ASSISTANCE COMMISSION, *supra* note 94.

97. *See id.*

98. "Do not expose the official registry file to the Internet," the study further states. "Create a copy of your authoritative database to use for your voter information Web site and regularly update it from the authoritative database." The study also counseled that personal information that is exposed when answering voters' questions also should be limited to what is "necessary and appropriate." The authors recommended encrypting the link as an additional safeguard. *Id.* That these basic database understandings constitute major recommendations of a December 2008 EAC study suggest that many states lack even a modicum of appropriate technical knowledge for designing or procuring, and then maintaining, highly secure and reliable complex databases. Further, comprehensive, independent studies of statewide voter-registration databases need to be undertaken immediately to document and address the risks to voter's franchise rights posed by technological malfunctions and design deficiencies.

99. Published Monday, Dec. 15, 2008: http://www.riverfallsjournal.com/articles/index.cfm?id=18614&section=Wisconsin%20News&property_id=18.

100. Ohio's 2008 federal litigation concerning the statewide voting registration database ended with the U.S. Supreme Court's short *per curiam* opinion, *Brunner v. Ohio Republican Party*, 129 S. Ct. 5 (2008).

101. States in which major technological research firms and academic institutions are located, such as California and Washington, appear to be managing their statewide databases significantly better than others, but they should not be taken as the national norm.

102. In an effort to improve its problematic election administrative record, Ohio's most populous county, Cuyahoga County, appointed an election monitor to facilitate compliance with best practices in elections and with governing law. As part of its work, the monitor submitted a report on the 2006 general election, identifying administrative tasks where indicators of legal noncompliance had come to light. Technical issues, including computer security practices, formed a major part of the report. In reviewing the voter

registration issues, specifically those regarding possibly erroneous voter registration deletions, the report referenced potential legal violations of the Voting Rights Act, 42 U.S.C. § 1971(a); the National Voter Registration Act, 42 U.S.C. §§ 1973gg-1 *et seq.* and especially § 1972gg-6; the Help America Vote Act, 42 U.S.C. § 15483; and Ohio voter registration statutes, OHIO REV. CODE §§ 3503.11–3503.33. After the monitor's report became public and executive leadership changed, the elections staff redoubled efforts to achieve electoral legal compliance.

103. See *supra* note 76.