2012

Voting Technology and the Quest for Trustworthy Elections

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

2012

Voting Technology and the Quest for Trustworthy Elections

S. Candice Hoke, *Cleveland State University*

CHAPTER 17

VOTING TECHNOLOGY AND THE QUEST FOR TRUSTWORTHY ELECTIONS

CANDICE HOKE

Over three decades after voting systems first incorporated software and computer chips,[1] and almost a decade after federal legislation impelled nationwide adoption of electronic computer-based voting equipment,[2] significant performance deficiencies undermine voters' and electoral officials' confidence in the reliability and accuracy of voting equipment. This conclusion may seem inexplicable given some notable achievements in the voting systems regulatory system. A relatively robust federal testing and certification apparatus has been created to subject voting systems to pre-market technical evaluation;[3] heightened standards and rigorous testing procedures for reliability, accuracy, and other essential attributes of the voting systems have been implemented.[4] Further, rates of voter error as measured against established metrics have sharply diminished, presumptively attributable to the federally required notice to the voter and an opportunity to correct the ballot before casting it.[5]

Nevertheless, more than 98 percent of Americans voting on 2012 election days will cast ballots on precinct e-voting machinery that has not been federally tested and certified in compliance with the 2005 standards.[6] Additionally, 2012 absentee ballots will similarly be tabulated on equipment that pre-dates the federal certification standards and testing system, although most absentee ballots will at least produce a voter created record that can be recounted or audited.[7] While federally certified voting systems have been marketed since 2009,[8] state governments lack the funding to upgrade their voting systems.

If the federal certification of these aging voting systems were merely perfunctory, providing a gloss but little more, the certification omission would arguably be acceptable. Unfortunately, nationally prominent independent computer experts have repeatedly documented that all but a tiny fraction of the equipment currently deployed manifests grave design, performance, and security issues that can produce inaccurate vote totals.[9] They have cautioned that the software's design and coding deficiencies combined with vendors' noncompliance with good industrial practices mean that no scientific basis exists for trusting the election results the equipment produces.[10] Additional quality assurances techniques are needed to verify the machine results, but few jurisdictions have mandated these steps.

Problems surfacing in actual elections tend to prove that the scientists' assessments are not merely theoretical projections.[11] Yet the vast number of ballots in 2012 and into the foreseeable future will be cast and tabulated on this gravely flawed voting equipment.[12]

When Congress enacted the Help America Vote Act of 2002 (HAVA),[13] creating the bipartisan U.S. Election Assistance Commission (EAC) charged with improving election administration and enunciating minimum standards for voting systems used in federal elections,[14] undoubtedly legislators expected substantial improvements over the punch card technologies that had caused the *Bush v. Gore* debacle. But the EAC faltered repeatedly during its first decade, from both misjudgments and calculated attacks.[15] As this chapter goes to press, the EAC's existence remains in question despite its assigned statutory role in voting technology regulation.[16] With the EAC's future and the federal role in regulating election technologies threatened,[17] this chapter seeks to provide an impartial examination of the legal, scientific, and regulatory structural issues embedded in the widespread use of problematic voting technologies.

This chapter reviews four dimensions of the still-unresolved voting technology quandary. It begins by briefly reviewing the Florida *Bush v. Gore* background that, combined with the tradition of state governmental control over election administration, spawned the contours and limitations of new federal regulatory apparatus. It also surveys some illustrative voting system malfunctions and their consequences surfacing predominantly from 2009–12. Thus, the first part of this chapter, *Background: Performance Records of Deployed E-Voting Systems*, commences where the 2009 edition of *America Votes!* chapter on voting technology ended.[18]

The second part of this chapter, *Federal Compulsion to Adopt Software-Based Voting Technologies*, explains the misconceptions about software and digital equipment that led to both the flawed federal mandates and the ineffectual regulatory structure.[19] These misconceptions continue to inhibit creation of a regulatory structure and substantive requirements that function effectively to protect the voting technology component of the fundamental right to vote. This part argues for a more robust and technically well-informed federal-state partnership in regulating voting technologies and their use.

The third part of this chapter, *Litigation and Enforcement Strategies*, focuses primarily on the curious omission of Federal enforcement of HAVA's voting technology standards. HAVA expressly vests enforcement powers in the U.S. Department of Justice.[20] This part also considers private party litigation that has sought to invalidate the use of allegedly defective voting machines.

The final part of this chapter examines *Federal Promotion of Problematic Internet Voting.* Despite the essentially unanimous warnings of the computer security community in the United States that Internet voting cannot achieve accurate vote counts or permit a trustworthy recount, some federal policy makers have pursued online voting. Because these systems cannot be secured by any known or foreseeable technology, they present the grave danger that remote cyber attackers could silently change the outcomes of Internet elections without officials able to detect any problem. While some state and local governments appear to have learned that a skeptical approach to vendors' overwrought marketing literature and field performance may be warranted, an obscure federal agency has been falsely contending that the U.S. Department of Defense has backed Internet voting. The Federal Voting Assistance Program (FVAP) has developed both carrot and stick approaches to urge states to modify their election laws to permit online return of voted ballots for overseas military and civilian voters. This section also examines the agency's claims that its actions fulfill rather than violate federal law.

The chapter concludes by advancing recommendations for preparing the legal system to realize voting rights despite the wide deployment of problematic voting technologies. Once we accept that the existing equipment is finicky rather than reliable, and that it is subject to tampering and tabulation disruption that may be undetectable without special skills and procedures, what should follow for the legal system? The legal presumptions thus far tend to assume accuracy of election totals and place the onus of proving a technical problem or tampering on a candidate. Requiring election equipment to provide extrinsic corroboration of electronically produced election results, or "evidence-based elections,"[21] better accords with the courts' role in assuring fundamental rights to vote.

Background: Performance Records of E-Voting Systems

SOUTH CAROLINA 2010

South Carolina's experience in 2010 serves as one recent exemplar. Reviews of the state's vote records generated in the Democratic Party statewide primary and the November general election documented legitimate bases for questioning the accuracy of the automated vote totals reported by the direct recording electronic (DRE) touchscreen[22] voting devices and tabulation software.[23] A virtual unknown catapulted to apparent victory in the Democratic U.S. Senate primary over a widely supported and well-known candidate, perplexing many seasoned consultants and political insiders. Oddly, the vote margins differed dramatically depending on how the votes were cast. The paper absentee ballot vote margins differed substantially from the reported Election Day e-voting machine totals, in a manner sharply divergent from other statewide Democratic primary races.[24] Election experts then documented a range of other anomalies that some, but certainly not all, commentators considered possible evidence of malfeasance or software bugs.[25]

The November 2010 general election added to South Carolina's concerns over electronic vote tally accuracy. Computer scientists working with the state's League of Women Voters gathered county ballot records to show that the legally certified election totals were erroneous. They demonstrated that county tabulation processes had somehow bypassed numerous voting machines' vote totals, effectively disenfranchising hundreds if not thousands of voters.[26] Their independent audit of county election tallies showed that the announced election results had excluded more than

300 votes from some candidates' totals.[27] But in addition to not tallying some of the electronic DRE touchscreen machines, one county's records reflected a count of 1,400 more ballots than actual voters.[28]

How could these tabulation errors remain invisible to conscientious election officials? The manufacturers often suggest "human error" rather than any fault in their voting system products.[29] But a closer evaluation shows the manufacturer had not designed the tabulation software to alert officials when some voting machines' vote tallies had been *skipped* and remained omitted from the overall election tabulation. Equally bizarre, the manufacturer did not design the voting system to report when one machine's tallies had been uploaded and added into the final tabulation *more than once*, thus according some voters more than the promise of one person, one vote. The software could easily have included the fail-safes of blocking the ability to close the election and report final vote totals if the tallies of any voting machines activated for the election had not been included in the final tally, or if any had been included multiple times. But the software designers did not include these mission-critical features—and no regulation or voluntary standards mandated them.

To complete the serious design omissions, manufacturer ES&S—the largest and one of the oldest election equipment vendors nationally[30]—did not recommend post-election auditing methods for verifying that every valid ballot cast had been reflected in the tabulation and that none were counted multiple times.[31] Not surprisingly, with no indicators otherwise, the local election officials reasonably believed all votes had been tallied, and the State Election Commission certified the vote totals as accurate.[32]

Unfortunately, South Carolina's experience with problematic electronic voting equipment is not aberrational. The ES&S "iVotronic" DRE touchscreen equipment[33] used pervasively in South Carolina lacks a paper record of the vote choices yet is deployed nationwide. The performance of the iVotronic machine and its central software have generated many electoral controversies, including some high profile litigation.[34] Whether using vendor ES&S's voting equipment or others', election offices have experienced a broad range of serious issues with e-voting systems. All-electronic DRE touchscreen units that produce no contemporaneous voter-verified paper record have received the most pointed criticism. The most widely endorsed e-voting systems require voters to mark a paper ballot that is then read by an optical scanner with vote tallies produced by potentially flawed software.[35] But these systems permit the extrinsic paper record to be used to verify or correct the software-produced vote tallies in post-election audits or recounts.

Elections conducted on e-voting equipment that HAVA financed have continued to experience inaccurate counts, unreliable performance, and other deficiencies from 2005 through 2011 regardless of the vendor, the type of equipment, the size of jurisdictions, and other factors.[36]

ILLUSTRATIVE E-VOTING EQUIPMENT DEFICIENCIES

While South Carolina's 2010 voters endured particularly searing experiences with their voting technology in both the federal primary and the general election,[37] South

Carolina is by no means unique. A national survey of irregularities demonstrates that no one equipment type or currently marketed brand or vendor can be singled out as either above the norm or well below the norm for serious technical problems. This section reviews a wide assortment of these serious issues arising in actual elections.

Turning first to a 2011 local election race in New Jersey, a supposedly losing but highly favored candidate suspected that the candidates' names were not correctly associated with the on-screen "buttons" a voter used to select candidates, causing swapping of vote totals.[38] In a lawsuit to investigate, the Fairfield County official acknowledged her programming "error" of mis-mapping buttons to the Zirkle and Henry candidates, leading to the official announcement of the wrong candidates as winners. The state judge ordered the computers that configured the election impounded for reviews by Princeton University computer and voting system expert Professor Andrew Appel, to confirm or clarify whether this explanation sufficed.

But Appel's scheduled arrival to assess the relevant log files somehow proved to be too late. Appel discovered that despite the court order to preserve the evidence, the logs and a vast amount of other system information had been erased the day prior to his evaluation, essentially tampering with evidence that might have revealed tampering with the election.[39] He had previously testified and written reports documenting the ease of tampering with voting systems' vote totals,[40] but other witnesses had ridiculed the likelihood that this could or would occur.[41] Nonetheless, within a matter of months, Appel's warnings arguably had been validated.[42]

In the 2010 general election in Saguache County, Colorado, several types of malfunctions undermined the trustworthiness of the reported results generated by the central office's scanner-tabulator system. "Every time we ran the ballots through the machine, it resulted in different numbers."[43] Additional machine malfunctions prevented the officials from complying with legal requirements to protect the election's integrity and assure its accuracy. The Canvass Board ultimately concluded that it could "not attest to the accuracy or inaccuracy of the returns."[44] Thus, the core election mission—producing accurate vote totals—could not be fulfilled, largely because of a range of voting equipment failures at mission-critical junctures. Notably, the same model of central count, high-speed optical scanner is one of the most broadly deployed central-count scanners nationwide.[45]

Cuyahoga County, within which Cleveland is located, is Ohio's most populous county. It postponed its transition to HAVA-approved e-voting until May 2006, but still found the demands of the primary too great. The absentee ballot system tabulation system failed, requiring a 24-hour hand count for almost a week. Every managerial system also failed, producing a notorious debacle.[46] Over the next three years, the county used three different e-voting systems and two different vendors, and it experienced major problems with each. But the election officials learned to distrust marketing claims and to check closely for performance quality.[47] When the county finally received one of the first EAC-certified precinct-based scanning systems, it proceeded critically. Cuyahoga County officials then discovered a range of issues, including that the equipment could not accurately count ballot choices in one column on extra-long ballots, although it had been marketed and certified for using extra-large paper. The county officials discovered a total of three additional serious failure modes that affected vote total accuracy or security and reported them to the EAC.[48] The EAC investigated and "substantiated" the three defects, promising to continue its work.[49]

In the 2008 primaries, a wide range of system irregularities and unexpected tabulation events occurred. For instance, on Super Tuesday, Senator John McCain's campaign had predicted an easy victory in the candidate's home state of Arizona. But Cochise County's initial tallies reported that challenger Mitt Romney had won. Local election officials examining the county tallies noticed a strange outcome: the tabulation software reported total votes that exceeded the total number of registered voters in the county. The officials then discovered that the software had counted the ballots of five large precincts not once each, but five separate times, thus generating an outcome of "one person, five votes" for those digital enhanced voters. "It was a cumulative (computer) error that just kept adding the results for five polling places every time new figures were added," explained the county official.[50]

One month later, Ohio held its 2008 presidential primary on March 4. The statewide weather of unseasonable freezing rain and snow proved the smaller of the major headaches facing suburban Butler County, near Cincinnati. While the tabulation software reported all precincts and memory cards had been tallied as part of the vote totals, election officials discovered that two memory cards and 105 ballots had somehow not been tallied. Curiously, the election software did not report the error, however, but instead had noted all votes were tallied. More troubling, county election officials discovered the memory card omissions only adventitiously, while examining the system's tabulation database for a completely unrelated reason. In their subsequent complaint letter to the vendor, Diebold, the local officials stressed their dismay that the software was capable of false representations that all votes were recorded and reported accurately.[51] Eventually, the vendor issued a "Product Advisory Notice" that acknowledged a software flaw that could lead to unreported failures in recording and tabulating votes, a flaw that affected all versions of the GEMS tabulation software stretching back a decade.

These vignettes relate only a small fraction of the errors occurring nationally in real elections with the current e-voting equipment.[52] No comprehensive inventory collects all irregularities and serves as a library for election officials and public consultation.[53]

Legal explanation of the status quo ineluctably requires a return to the pivotal Florida 2000 presidential election and its aftermath. The congressionally perceived urgency behind forcing nationwide adoption of these relatively untested e-voting systems requires returning briefly to *Bush v. Gore*[54] and its aftermath. In the decision's wake, the nation demanded improvements that would obviate any repeats of the underlying punch card calamity. Congress translated these goals into a wide range of explicit requirements for federally financed voting systems deployed in all federal elections no later than 2006. HAVA required all voting systems to attain an exceptionally high accuracy rate[55] and permit manual audits.[56] While HAVA did not specifically mandate electronic voting systems, virtually the only equipment deemed able to satisfy the new functional mandates entailed software and computer chips.

FLORIDA 2000

As the November and December 2000 days wore on post-election, the nation and its judiciary learned that the aging equipment used for recording and counting votes erred at the average rate of two percent of all ballots cast.[57] While narrow election margins in Florida and elsewhere were not unusual, it was unprecedented that the Electoral College's national determination of the presidency would depend on whether some counties would be permitted to conduct a manual recount of ballots. On December 12, 2000, the U.S. Supreme Court decided to halt the recount ordered by the Florida Supreme Court, ruling that the state court had authorized a recount that could not achieve the protections against arbitrary and disparate treatment afforded by the Equal Protection Clause.[58] The Court's ruling ended the Florida recount and in effect determined the race between George W. Bush and Al Gore for the presidency.[59]

While the legal questions vexed the public and the courts,[60] the voting technology itself assumed major role in the overall drama. During the legal and political controversy and during the congressional inquiries thereafter, the punch card equipment came to be viewed as one of the chief villains of the 2000 election. The persisting controversy ushered in the contemporary era of distrust of voting technologies' accuracy. Not unsurprisingly, after the U.S. Supreme Court had effectively become the presidential race tie-breaker because of voting equipment issues,[61] Congress initiated rapid replacement of punch card, lever, and other existing voting systems. The federal legislation required the voting system to be able to alert voters when either of two voting "errors" occurred: the voter's failure to record any vote in a race (undervote) or the voter's selection of too many votes in a race (overvote). These "second chance" voting systems accord the voter timely notice of errors and an opportunity to fix the problem before the ballot is irretrievably cast.[62]

By 2006, the federal statutory and funding initiatives resulted in the vast majority of American voters casting ballots on computer-based equipment.[63] After overcoming the transition difficulties from the old voting systems, in the 2008 and 2010 election cycles jurisdictions achieved certain measurable improvements, especially in reducing "overvoting" and other voter errors.[64]

But the nation has thus far not broadly benefited from the substantially improved standards and certification process. By early 2012, over nine years after statutory enactment and four years after the first federal technical standards had been generated by the new federal EAC, no more than 12 of the over 7,000 election administrative jurisdictions are conducting elections using EAC-certified voting equipment.[65] Most U.S. election jurisdictions continue to use voting equipment that lacks federal certification by federally certified independent labs that use approved testing methods. Instead, the equipment was "qualified" under weak testing procedures supposedly complying with the earlier minimal standards issued by the Federal Election Commission prior to the creation of the EAC.[66] The scientific evidence demonstrates that this equipment is far easier to rig for widespread and largely undetectable cheating than the punch card and lever equipment it replaced. This profoundly insecure voting equipment continues to be deployed in 2012,[67] however, partly from lack of funding to replace it and partly from lack of significantly improved options. Thus, the federal quest to eliminate fallible voting technologies,[68] born in the aftermath of the Florida 2000 presidential election, remains unachieved in the midst of the 2012 election cycle.[69]

Even though voting technology legal and regulatory issues garner less media attention than voter fraud,[70] voter identification, and vote suppression issues,[71] these matters are central to voting rights protection and popular sovereignty.[72]

Federal Compulsion to Adopt Software-Based Voting Technologies

Is it possible to develop a voting technology that records and tabulates votes in an accurate, completely impartial manner regardless of inadvertent human error (by voters and officials) and deliberate tampering? Can the system also be designed to be responsive to all voters despite their presenting a diversity of languages, levels of literacy, and life situations, while also providing sufficient ballot secrecy to exclude possibilities for vote buying and coercion? After the controversies generated by the 2000 presidential election, political scientists, government officials, and election advocates converged on a more or less common vision of an impartial, provably accurate, tamperproof, and consistently available election machinery for recording and tabulating votes—a technological "Archimedean point."[73] HAVA became the vehicle for realizing this technological vision.[74] HAVA's proponents expected the market to respond to over $3 billion in federal funding by producing computer-based, automated equipment that attained their idealistic objectives.

HAVA

Encouraged by vendors' representations, Congress envisioned an election administration regime where the newer electronic voting equipment would expunge inadvertent human error and deliberate mischief from the voting process, regardless whether committed by voters or election staff. Vendors assured the representatives that new digital voting systems could attain previously unachievable accuracy and speed in both vote recording and election results tabulation, reducing the error rate to a level substantially below then-current punch card voting technologies discredited in the Florida 2000 election.[75] Because the information technology industry had automated seemingly similar tasks, the goal of automating elections on an expedited timetable appeared straightforward. Little attention was accorded to whether and in what ways elections differed from prior contexts.[76]

But congressional antipathy for creating another federal agency was intense, especially within a historic bastion of state power. Combined with the then-prevailing faith in the market, the compromise version of HAVA provided for an unusually weak Election Assistance Commission. Congress granted the EAC the power to disburse funds and to implement other HAVA sections that mandated research and clearinghouse functions, but did not vest the EAC with any regulatory power.[77] Instead, Congress charged the EAC predominantly with the role of providing "guidance" via "best practices" and "voluntary" standards for state election systems.[78]

Although the U.S. Constitution authorizes Congress to "make or alter" the states' rules concerning the "Times, Places, and Manner" of holding federal elections,[79] states have zealously sought to protect their control over election administrative processes. In the development of HAVA and the EAC, state governments stressed the federalism dimensions of elections and argued for no new federal powers to be conferred on a federal agency.[80] To date, Congress has not delegated to a federal agency regulatory power to mandate state compliance with a set of federal minimum standards for voting equipment.[81] Congress had arguably vested in the Federal Election Commission (FEC) some advisory responsibility over technologies used in elections, but only to generate guidance, not to impose mandatory performance standards.[82] HAVA transferred FEC's limited authority to the new Election Assistance Commission, and directed development of new voting systems standards with the participation of independent technical experts, National Institute of Standards and Technology (NIST) experts, some election officials, disability accessibility experts, and others.[83] But these standards were again voluntary, not mandatory, even for voting systems used in federal elections.

Importantly, however, Congress did not defer all voting technology standards to the voluntary "consensus" approach. The 2000 election convinced lawmakers that voting systems must attain a much higher degree of accuracy and reliability than the antiquated, predominantly mechanical technologies. HAVA described functional features the new technologies should incorporate but refrained from requiring that all voting systems meet minimum federal technical standards other than those specified directly in HAVA. Thus, the Act expressly requires all voting systems used in federal elections to include a manual audit capability, and it proscribes rates of error in counting votes above a specified minimum.[84]

But HAVA was not the source for the regulatory and certification testing apparatus for the vast number of voting systems in use from 2004 through 2012.[85] Because the HAVA-mandated voluntary voting system guidelines and certified testing laboratory system could not be achieved quickly but HAVA mandated deployment of the federally funded voting systems no later than 2006, virtually all HAVA-funded voting systems have not been certified under the EAC's 2005 standards. HAVA's rapid deployment requirement effectively left in place the weak standards and lax certification process of the "qualification" testing system established by FEC and the National Association of State Election Directors (NASED).[86]

The weakness of FEC's efforts to develop publicly protective voting systems standards for computer-based voting equipment may be partly attributable to Congress's omission of express delegation of regulatory authority. The FEC's original standards development began in 1984, with issuance in 1990.[87] Although the FEC began updating in 1997[88] and issued a revised set of standards in 2002,[89] they were known from the outset to contain weaknesses in security, auditability, usability, and system reliability.[90] This NASED-FEC testing regime's structure did not lead to consistent compliance testing, as the vendors directly contracted with the labs they preferred and thus were the paying customers of the labs. The labs did not maintain an appropriate arm's-length distance from the vendors. Several studies suggest that the labs performed substantially less than the minimal testing required even under the FEC's weak 2002 standards.[91]

HAVA also did not specify a compliance system for ensuring that voting equipment and voter registration systems would satisfy the mandatory statutory standards when fielded in real elections. This omission and its consequence—of no data to demonstrate the equipment's malfunction and miscount rates—may be one reason that neither the U.S. Department of Justice nor private citizens[92] have sought to enforce HAVA's auditability and accuracy standards.[93] Unlike data collection under the National Voter Registration Act, HAVA did not require independent verification of compliance with the statutory standards. Congress appeared to be persuaded that computer-based voting machines would resemble slightly re-configured banking technologies (such as ATMs) and thus presumably highly accurate and secure. Unquestionably, HAVA's reliance on the market reflected the then-prevailing congressional faith in the capacity of private companies to produce high-quality products at lower prices than a scheme of mandatory federal regulation.

The market, however, did not produce equipment fully compliant with HAVA's specified requirements, or with the ideal of nearly perfect election equipment. Independent scientific assessments of voting systems have identified numerous, gravely problematic design, implementation, and procedural flaws and outright defects in current voting equipment.[94] Field performance records in actual elections have confirmed these flaws and their implications for voting.[95] These include defects in both software and hardware that can be deliberately exploited to manipulate results, often in undetectable ways.[96] Inadvertent software design defects generated from coding errors or "bugs" can also vitiate system security and data integrity.[97] Yet the flawed systems continue to be widely deployed throughout the United States,[98] largely owing to state fiscal conditions and lack of better alternatives.[99] Despite the independent documentation of serious deficiencies, with a few exceptions, the same flawed voting technologies from 2006 and 2008 will be utilized in the 2012 presidential cycle.[100] Thus, in the 2012 presidential election virtually all Americans who cast ballots will have them tabulated on unreliable computerized equipment controlled by problematic software.

ELIMINATING THE HUMAN ELEMENT IN VOTE TABULATION

A largely tacit and highly contestable assumption has motivated the shift to software-based technologies for voting: whenever humans are involved in determining what marks constitute a valid vote, or what is the correct electoral count, concerns arise regarding possibilities of political bias and conflicts of interest that might result in a less-than-honest count. The quest for unequivocal and irrefutable election tallies has resulted in an effort to remove human judgments from the election system to the maximum degree possible. This conception seeks to substitute in place of humans a presumed impartial technological system for recording, tabulating, and reporting votes. With this system in place, supposedly the ultimate electoral objective can then be achieved: high public and candidate confidence in the results with virtually no need to question the actions of election officials.

Voting technology and computer security expert Professor Doug Jones has traced the reasoning: "The problem of interpreting voter intent when hand counting paper ballots has led many people, over the past century, to press for the use of impartial machinery in all ballot counting." Jones points to election recount disputes in the 2000 election cycle as evidence. The attorney for presidential candidate George Bush, James Baker, suggested, "Voting machines are not Republican and are not Democratic, and are not subject to conscious or unconscious bias."[101] Some of the proponents of this idealized view of an infallible technology include courts. The Eleventh Circuit observed,

> this vote counting model [is] the "machine model," because it counts as valid only those votes that the vote tabulating machine can read and record. The machine model thus relies on an *objective tabulating machine* that *admits of no discretion to count votes—if a vote is properly cast according to the instructions given to the voter, the machine will count it.*[102]

Cumulatively, these approaches contemplate a supremely objective electoral Archimedean point, an election technology that functions accurately and reliably to record and tabulate votes in a completely neutral and impartial manner, impervious to all manipulations. When measured against this benchmark, current election technologies unquestionably present grave flaws.

Professor Jones suggests that rather than the impartial neutral tabulator model of "vote counting systems," gambling machines provide the better analogy:

> Gambling machines, even such trivial machines as dice, can certainly be biased. Such biases can be accidental, the result of imperfect construction, or, as in the case of loaded dice, they may be deliberate. A voting machine may be biased in exactly the same ways![103]

Notably, with both tampering targets to the untrained eye, the tampering may be completely undetectable, leaving observers and participants believing that the machines—the dice and the software-based voting machine—are functioning accurately and neutrally. Unfortunately, dashing the dreams of HAVA's core sponsors and arguably some prominent jurists,[104] computer-based voting systems cannot attain the role of a neutral tabulator; numerous human tasks are required for it to function correctly, tasks that are susceptible to "(accidentally on purpose) mistakes."

Misconceptions of the capacity to exclude human judgment and roles from electronic election machinery supply a major reason for the continuing congressional failure to construct an adequate regulatory regime for assuring that voting rights are realized. This fifth point joins the four other reasons identified in the chapter of the previous edition of *America Votes!* that discussed national deployment of voting and database technologies whose reliability, security, and other technical properties were profoundly deficient.[105] First, the HAVA-mandated regulatory activities were not sequenced properly for the best use of the federal monies, as the funding mandated procurement and deployment before the standards and testing regime had been launched. 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. The voting system vendors engineered only minor adjustments to their existing product line, and then rushed their products to market on the compressed HAVA-specified timetables. 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 into software-based voting systems, instead apparently assuming the market would satisfy all needs. Finally, Congress's prevailing faith in the market to produce outstanding election equipment constituted the fourth major regulatory mistake. The voting equipment market's defects include substantial market concentration and few market players. Significant barriers to market entry and an artificial "market" comprised exclusively of state and local governmental purchasers mean that it is not possible for a "free market" to exist; it does not partake of any of the essential features of a free market. Where governmental entities are the sole buyers, normal market dynamics cannot operate. The nation and the voting system vendors might be better served by considering a public utility model.

THE EAC'S FUTURE

Over 2011, the National Association of Secretaries of State (NASS) resumed work on its goal of terminating the EAC.[106] As stated by the Senate bill's sponsor, the asserted justifications include contentions that no set of election problems persists on which its work is needed; voting system certification is unworkable because of costliness and delays in approving new systems and software patches; and the EAC's spending objectives are unimportant.[107] Early in 2012, NASS surprisingly urged resumption of the EAC Boards' activities, suggesting that perhaps the organizations' members have recognized some significant losses would occur if the EAC were abolished.[108]

Over two-thirds of the states by law depend in some manner on the EAC-voting system and testing lab certification system.[109] Zeroing out the funding would immediately leave the states and the voters without the testing lab supervision, ongoing work updating voting system standards, and maintenance of the "clearinghouse" library of research and best practices relating to election administration. While the public record is thin, one explanation for the vendors' antipathy for the EAC lab testing system lies in its greater rigor in identifying serious flaws in the software and hardware that could undermine the systems' accuracy, security, auditability, or reliability.[110] Because the vendors have tended to use the certification labs as their beta testing units rather than engaging in proper design and pre-certification testing,[111] the testing labs have faced a much more arduous and time-consuming set of tasks than expected. But vendors have not publicly revealed their system failures caught by the certification labs, and need not since the labs do not generally report the range of flaws found over the entire testing process if the vendor fixes the problems to the lab's satisfaction. Instead of upgrading voting system quality, the industry has sought to weaken the testing apparatus and the standards-setting bodies, and recommends against imposing design standards, despite the most significant deficiencies occurring at the design level.[112]

Given the constitutional importance of elections and voting rights, and the inability to design and manufacture voting systems that do not depend on insider humans—who may be biased or incompetent—having special access, the EAC's work in the voting systems arena and in data collection is too publicly valuable to be forsaken in a cost-cutting effort. Unquestionably, the agency needs substantial structural and operational reform, and expert computer security staffing, to meet the current challenges election administration faces.

Litigation and Enforcement Strategies

Structural litigation challenging the adequacy of voting technologies for assuring franchise rights largely began with the 2000 Florida presidential race. While *Bush v. Gore* arose in the context of a disputed election, subsequent litigation has overtly sought structural reform.[113] In the watershed case, the Supreme Court critically examined whether the state government had discharged its duty to realize franchise rights, which in turn spurred HAVA's enactment and state legislative reforms.[114] This section provides a relatively brief, high-level overview of litigation and enforcement opportunities by providing a typology that covers much of the litigation to date. It concludes by reviewing major powers and duties legislatively vested the U.S. Department of Justice (DOJ or Department) to ensure that deployed voting technologies do not impair voting rights and structural electoral legitimacy.

LITIGATING VOTING TECHNOLOGY DEFICIENCIES

Voting machines, whether electronic or mechanical, are merely tools to facilitate casting ballots and counting votes, a means for achieving the popular sovereignty guarantees of the Constitution.[115] At bottom, litigation against certain electronic voting systems—paperless DREs in particular—claims that the tool generates sufficient risks and potential deprivations of rights that the equipment should be legally invalidated. Notably, the litigation need not (and should not) request a judicial order of specified preferred technology as that question lies beyond judicial competence. Specification of legally compelled minimum requirements to be met—for instance, a software-independent record of each cast ballot—is sufficient to permit the state's administrators to proceed.[116]

While the U.S. Supreme Court has not maintained consistency in whether an individual rights paradigm or a structural interests paradigm (focused on systemically fair elections) should ground election litigation, when facing a constitutional challenge courts tend to use the individual rights lens.[117] The Supreme Court leans toward the individual rights approach, but the structural approach probably best fits the nature of the wrong and the rights in jeopardy.[118] In virtually all electoral contests, an individual's votes and the votes of other eligible voters need to be recorded accurately and then accumulated, tabulated, and reported as one tally reflecting all cast ballots. If the voting machinery is seriously flawed in ways that render some votes not safeguarded in all requisite steps, the accumulated totals may be affected in ways that legally amount to systemic deprivation of rights to political self-determination via elections for representatives. Voters thus inherently have an interest in the systemic attributes of the election, as their votes are meaningful only when accumulated.

Although voting system litigations often arise in the context of a disappointed electoral result, this review sidesteps election contests in favor of systemic, structural litigation.

Breach of Contract, Product Liability, and Warranty Claims. In a breach of contract or warranty action, normally the government entity that purchased the equipment files suit against the vendor. But the norm is breached often. For instance, an acrimonious Ohio action began when Premier Election (the former Diebold Corporation election division) brought suit against the state of Ohio and several Ohio counties for a declaratory judgment that the company had met all of its legal obligations.[119] The Secretary of State counterclaimed for breach of warranty, breach of contract, and fraud in the inducement.[120] In advance of the filing, the parties had exchanged written claims and had been conducting settlement negotiations that the Secretary expected to continue. But the vendor rushed to file first in its preferred venue. The Secretary of State returned the favor by issuing a press release announcing the state's counterclaim for "voting system malfunctions" in 11 of the 44 counties using the company's voting system. The statement explained that the malfunctions resulted in dropped votes when memory cards were uploaded to the server, without effective notice to the election officials.[121]

Other election jurisdictions that have maintained successful breach of contract and warranty lawsuits include San Francisco[122] and Montgomery County, Pennsylvania.[123]

Voting Rights Act. Challenges to the adequacy of voting systems have been maintained under Sections 2 and 5 of the Voting Rights Act (VRA).[124] Courts have recognized two separate analytic categories under Section 2, specifically "vote denial" and "vote dilution."[125] As Professor Dan Tokaji succinctly explains, vote denial embraces practices that prevent individuals from voting, such as poll taxes and literacy tests. Vote dilution under the VRA identifies unlawful restriction of the political influence of minority groups.[126] Section 5 requires preclearance of proposed modifications of voting systems for "covered" jurisdictions.[127] Both courts and scholars have honed these claims during the nearly five decades since the Act's passage.

Fourteenth Amendment: Equal Protection Clause and Substantive Due Process. Following *Bush v. Gore*, numerous cases have challenged aspects of voting technologies on equal protection and substantive due process grounds. In Ohio, the Sixth Circuit determined that the structural claims of *Stewart v. Blackwell*[128] and *League of Women Voters of Ohio v. Brunner*[129] (*Ohio League*) were properly embraced within the Fourteenth Amendment.[130] *Ohio League* ultimately resulted in a substantial multi-year structural settlement with particularized relief for the voting technology flaws.[131] Similar to Ohio's *Stewart* litigation, Illinois faced a combined equal protection and Voting Rights Act challenge to the use of punch card technology, primarily for differential error rates and disenfranchisement in the minority communities as compared with Caucasian voters. The district court ruled that no justiciability barriers obstructed the case from moving forward.[132]

The structural aspects of the *Ohio League* challenge to voting system adequacy are manifest in the Sixth Circuit's discussion:

> Jeanne White alleges that touchscreen voting machines utilized in Ohio violate her constitutional rights to equal protection and substantive due process. . . . White alleges that on November 2, 2004, she attempted to vote for president at her polling place in Mahoning County. That polling place utilized direct-recording electronic voting machines, more commonly known as touchscreen voting machines. White attempted to select the candidate she preferred, but the machine "jumped" from her candidate to another candidate. The machine "jumped" several times when White attempted to correct this problem. White believes that her vote may have been counted for the wrong candidate. *She also alleges that "jumping" occurred on other machines in Mahoning and other counties, causing votes to be counted for the wrong candidate. White seeks injunctive relief, in the words of the district court, "to ensure Ohio voting machines function properly in the future and can be audited for accuracy."*[133]

Winning a reliably accurate voting technology for herself or her precinct would do little to correct the harm to aggregative voting rights, for which all voters must have equal rights to cast ballots that can be counted accurately.[134] Solving voting technology issues at an individual level does not redress the structural problems generated by the voting system defects.[135]

State Constitutional Claims. During 2011, three states that use paperless DRE "all-electronic" touchscreen units for precinct voting faced major challenges based on state constitutional law. At this writing in March 2012, two cases are pending in state appellate courts and one decision was issued in 2011. In the Texas litigation, the state supreme court unanimously ruled that the state law had delegated to the Secretary of State the choice of whether some counties could use DREs that lacked a paper record.[136] The court did not discuss the possibility that under such a deferential standard of review, a political leader would be enabled to select voting machines that permit covert suppression or tampering with the votes of her party's opponents, thus assisting incumbents' maintenance of power. Nor did the court openly consider that political power over election operations could be used to create administrative rules that left vulnerable voting systems open to insider or remote programming for vote swapping.[137] The Texas court also seemed not to recognize the need for software-independent checks of the vote tallies to ascertain their accuracy. The court's selection of a highly deferential standard of review is inappropriate for the fundamental structural rights at stake and the ease of covertly abusing administrative power over voting systems in largely undetectable and untraceable ways. This judicial stance fails to protect Texas citizens' structural rights to elections with ballots counted as cast and fails to accord the citizens proof that their election tabulations are correct.

Litigation filed in 2004 challenged New Jersey's compliance with the state constitution's protection of voting rights. The case has contributed to multiple changes in state executive personnel and offices responsible for election technologies, but the state continues to defend its paperless DRE voting systems. After a long trial and a lengthy compromised decision on the merits, the court ordered the state to upgrade its physical security practices substantially.[138] When the state did not comply with the judicial orders despite numerous extensions and yet no sanctions issued, plaintiffs filed an appeal requesting that the decision be overturned. Plaintiffs have produced proof of the mis-mapping of candidate "buttons" to the database vote tables in a manner that covertly flipped the losers and winners in a real election, and have also documented unlawful deletion of election electronic records that were the subject of a court order.[139] This proof tends to confirm the plaintiffs' independent experts' assessments of real election consequences resulting from the equipment's deficiencies. Defendants had claimed the problems were "theoretical" rather than meaningful in real elections. The appeal is pending at the time of this writing.

In *Banfield v. Cortes*,[140] the plaintiffs' claim that the paperless DRE voting units used in much of Pennsylvania violate the Commonwealth's constitutional assurance of elections that will occur on equipment with "perfect" accuracy. The case has been appealed on the basis of cross motions for partial summary judgment. Because the independent experts' empirical assessments of this voting equipment demonstrate beyond cavil that the deployed equipment cannot produce accurate vote totals consistently, the court should validate the plaintiffs' claims.

ENFORCEMENT BY THE U.S. DEPARTMENT OF JUSTICE

The U.S. Department of Justice allocates civil enforcement of federal election law to its Civil Rights Division (Division). A subdivision, the Voting Section, maintains the primary election law expertise. The Division has posted on the Department's webpages a narrative of its pending cases and immediate past enforcement actions.[141] A close reading of this presentation, combined with a key word search of the DOJ webpages and a Westlaw electronic search of reported cases for the past decade, reveals that the Voting Section has generally avoided enforcement of HAVA's voting technology standards other than for assistive technologies for non-English language and physical accommodation.[142] Additionally, despite HAVA's compulsion of shifts to e-voting virtually nationwide between 2003 and 2006, and the resulting change in the types of records that would need to be maintained as evidentiary proof of election activities, DOJ has not undertaken the effort to reassess what electronic and related e-voting records need to be maintained to fulfill the purpose and letter of the Civil Rights Act of 1960 and other federal statutes.[143]

The Division's narrative overview of its HAVA enforcement activity includes attention to bilingual ballots, protection of the Puerto Rican voter, and accessibility for disabled voters—all of which are vitally important, legally compelled objectives that can be characterized as classic civil rights enforcement of underserved minorities. But the question is why DOJ has selected some parts of HAVA for enforcement and yet has systematically neglected the voting technology minimum standards articulated in HAVA's Title III. These include accuracy standards in vote recording and tabulations,[144] an auditable manual ballot, privacy, and other foundational protections of systemically fair elections.

Thus far, through both presidential administrations since HAVA's enactment, DOJ has proceeded timorously rather than assure realization of the basic prerequisites for computer voting systems that Congress specified in HAVA. The extant public record suggests DOJ has largely sidestepped enforcing HAVA Section 301's more technical but mandatory[145] voting systems standards. This neglect arguably sends an implicit message to states, voting system vendors, and the public that DOJ views compliance with these standards as not worth the Department's efforts, perhaps to the point of mere hortatory verbiage.[146] Such a stance augurs poorly for realization of fundamental voting rights and warrants DOJ's rapid reconsideration.

Despite the dramatic transformation of election technology over the past two decades, the need for verifying vote tabulation accuracy and verification—that the announced totals actually reflect the voters' choices—has become more critical rather than less. Auditability, or extrinsic proof of the count, is a required component of HAVA.[147] Especially with software-based systems, manual auditability of a contemporaneously generated paper record constitutes the only effective check on the largely invisible, buggy software, and is thus critically important to the structural dimensions of voting rights. The Supreme Court has historically viewed the verification that voters' ballots have been correctly counted and reported as integral components of the fundamental right to vote.[148] Thus, marking vote choices on a ballot (whether electronic or paper) and successfully depositing it into a ballot box do not complete the scope of constitutionally protected voting rights. Instead, the Court requires that the subsidiary steps that ensure the right to vote is meaningful rather than illusory are legally protected. Thus, the constitutionally protected right to vote does not stop at the ballot box but encompasses the activities of accumulating, counting, and reporting the vote tallies.

The clearest delineation of these principles can be found in the numerous ballot box-stuffing cases. In *Gray v. Sanders*, the Court stressed that the right to vote encompasses the right to have the vote correctly counted as cast:

> Every voter's vote is entitled to be counted once. *It must be correctly counted and reported.* As stated in *United States v. Mosley,* "the right to have one's vote counted" has the same dignity as "the right to put a ballot in a box." It can be protected from the diluting effect of illegal ballots.[149]

Reynolds v. Sims[150] further elaborates these constituent principles embedded within the constitutionally protected right to vote:

> A consistent line of decisions by this Court in cases involving attempts to deny or restrict the right of suffrage has . . . repeatedly recognized that all qualified voters have a constitutionally protected right to vote, *and to have their votes counted.* In *Mosley* the Court stated that it is "as equally unquestionable that *the right to have one's vote counted is as open to protection . . . as the right to put a ballot in a box.*"

Note that the Court explicitly separates voting *participation*—which impliedly encompasses the citizen's right to receive a blank ballot and to mark and deposit it into a ballot box—from the right to have the vote counted. The Court does not create a constitutional hierarchy of the constitutive steps embedded in voting, and does not favor for particular protection front-end participation over the right to a correct count.[151]

Given the Court's delineation of integral activities encompassed within the fundamental right to vote, which are cumulatively designed to assure that all valid voters can vote and that their votes are counted correctly as cast, DOJ's narrow approach to enforcing the right to vote as ending with the depositing or casting of the ballot cannot be validated. The Court's precedents stressing the critical importance of votes being counted as cast and assuring that vote totals reflect the undiluted strength of each voter's choices means the DOJ must police the virtually invisible opportunities by which software-controlled voting systems can be exploited for denying voting rights. Fortunately, HAVA and other federal laws have already conferred the tools by which DOJ can fully protect voting rights on computer-based voting equipment. DOJ, however, needs to acquire technical knowledge and a courageous vision grounded in technical and computer security competence in order to assure the voting rights of all citizens.

The need for DOJ to reassess its enforcement tasks pertaining to voting technology has recently become more critical. In a summary proceeding, the Supreme Court expressed doubt that HAVA implies a private right of action to enforce a state's management duties concerning the HAVA-required statewide voter registration database.[152] Whether private citizens can enforce this or other parts of HAVA, including Title III's voting system standards, remains unresolved. HAVA explicitly authorizes

DOJ enforcement, however, of these "uniform and *nondiscriminatory* election technology and administration requirements."[153] Arguably, Congress delegated to DOJ not only the power but also the duty to enforce HAVA, especially where it implicates fundamental rights.

At least three reasons militate in favor of DOJ's acquiring the requisite technical capacity for interpreting and enforcing federal law relating to the performance of voting systems. First, the legal monitoring and enforcement of voting systems in some respects relate to the civil rights of all Americans, and thus function more analogously to the seminal redistricting cases that established the principles of voting strength equality. This historic line of cases, summed popularly as "one person, one vote," includes *Baker v. Carr*[154] and *Reynolds v. Sims*.[155] Voting technology enforcement relates both to the rights and interests of all citizens as well as to constituting a special interest for protecting communities historically suffering abridgement of their voting participation.[156]

As part of its civil rights enforcement for all Americans, DOJ must recognize the unpleasant potentiality that nullification of franchise rights, and consequently of democracy and popular sovereignty, can be caused by software bugs or deliberate covert tampering. The Department's recent record, however, suggests it has allowed itself to remain ignorant of the new cyber threats to voting and the covert tools that can be used to defeat electoral democratic self-determination and voting rights. Although voting rights can be secretly nullified, with technical tricks or bugs, only those with the correct skill set and understandings can uncover the exploits and protect voting rights. The election officials managing the election operations also are predominantly without cyber security training sufficient to allow them to protect against the obscure but effective vectors—both deliberate and inadvertent—by which electoral results can be modified and voting rights nullified. The nation can no longer afford its chief vindicator of voting rights to remain an ignorant and passive bystander. Strategies are available for DOJ to equip itself for protecting voting rights despite the use of software and complex technical systems, and for assuring that elections produce competent evidence of recording and counting votes accurately.[157]

The second reason for the Department to acquire voting systems with technical competence relates to DOJ as a party plaintiff where lawsuits or other legal activities are necessitated to protect voting rights. DOJ is unquestionably a proper plaintiff statutorily empowered to vindicate citizens' structural rights to fair elections as well as their rights to vote on devices that meet HAVA's minimum standards.[158] Technical competence is needed, however, to understand why many of the currently deployed voting systems arguably fail to satisfy HAVA and Fourteenth Amendment substantive due process protections,[159] and to exercise judgment in developing enforcement priorities. DOJ competence is even more critical given that the Court might hold the Department constitutes the only party plaintiff HAVA authorizes.[160] Its support of other litigation via amicus briefs and other activities could dramatically improve the protection of voting rights from technical deficiencies in voting systems.

Third, DOJ has not delineated guidelines for what types of electronic records of federal elections must be maintained pursuant to the Civil Rights Act of 1960.[161] The originating purpose of Section 1974 was to ensure that essential evidence is gathered and protected for DOJ to evaluate the lawfulness of an election process and the fulfillment of voting rights. This purpose, however, cannot be fulfilled unless DOJ lawyers learn of the types of records that e-voting systems can keep and how these records can be covertly destroyed or not gathered owing to operators (or vendors) disabling the record-keeping functions. DOJ needs to redress this decade-old omission with vigorous record-keeping standards that it also subjects to its monitoring powers.[162]

When one understands software and the multitude of opportunities it offers for mischief and malfeasance, avoidance of voting systems legal-technical issues cannot be viewed as a benign oversight. Because of the specialized expertise that is needed in an ongoing manner, a special DOJ legal team charged with full realization of the technical aspects of HAVA, the Voting Rights Act, and the Fourteenth Amendment protections of voting may be warranted. Fortunately, some preeminent computer scientists have developed expertise in voting systems and a facility in teaching the basics to those who lack the scientific background, and could be tapped to assist DOJ in fulfilling its critical civil rights role in the age of digital voting.[163]

Federal Promotion of Problematic Internet Voting

In the late 1990s when precinct-based electronic voting systems were gaining a foothold in urban locations, a small unit within the U.S. Department of Defense (DoD) became convinced that military and overseas civilian voters would be best served by moving their election activities to the Internet. Unlike the e-voting systems HAVA funding spread throughout the nation that had been designed and deployed with little advance review from computer security experts, the Federal Voting Assistance Program's (FVAP) fanciful plans have received sustained critical attention. But despite emphatic and nearly unanimous refutation of the claims FVAP advances, FVAP marches to its own drummer, refusing to heed the consensus of independent computer security experts that it should drop or dramatically scale back its planned Internet voting initiatives given expanding and unpreventable serious cyber security threats to United States interests. FVAP has also offered millions in grant monies for states to experiment with proto-Internet voting technologies, despite the lack of any independent testing and validation of such systems before funding their procurement. A considerable scientific literature concludes that Internet voting systems present enormous, technically unmanageable threats to the integrity of elections and to the legitimacy of the results. At least in the federal election context, the danger rises to the level of a threat to U.S. national security. FVAP's activities also arguably violate governing election law, yet persist because of the agency's decade-long embrace of this vision of all-electronic, paperless elections and agency leadership issues.

Unquestionably, American military and overseas civilians have faced significant obstacles to casting valid absentee ballots in U.S. elections. State governments have historically designed their absentee rules for domestic voters temporarily absent from their homes on Election Day. The voting needs of those either in combat zones or living as long-term residents of foreign nations have until recently largely escaped state attention. Military personnel who change their residence frequently have historically found the absentee balloting processes complex and confusing, imposing barriers to casting valid ballots. In some cases, the state rules had erected almost insuperable barriers to overseas voters, such as requirements for notarized ballots.[164]

The federal government has been particularly concerned with redressing the procedural impediments to voting that uniformed service members face.[165] While recognizing our electoral system's federalism tradition, Congress has attempted in several enactments to eliminate state hurdles and thereby facilitate military and overseas voting.[166] By enacting the original Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) in 1986 and then amending it in 2009's Military and Overseas Voter Empowerment Act (MOVE Act),[167] federal law no longer simply encourages states to reconsider absentee voting obstacles but now also bars certain practices. The MOVE Act seeks to ensure that UOCAVA voters will have sufficient time to complete all tasks requisite to voting, including voter registration, receipt of blank ballots, and return of voted ballots in a timely manner. By statute and Executive Order,[168] the DoD, and in turn, the DoD's FVAP, have been delegated the federal duties for facilitating UOCAVA voting.

This section reviews the federal legislation and FVAP's activities that relate to voting technology. Unfortunately, FVAP has arguably not executed its duties consistent with governing law and in some respects has significantly undermined state and local capacity for conducting elections that are secure against remote hacking. Although federal statutes specify a series of affirmative steps to remedy UOCAVA voters' low voting participation rates, for at least a decade FVAP has not focused on its assigned duties but has set its priorities based on a naïve and technically unsophisticated view that software and Internet-based technologies can "solve" the problems faced by UOCAVA voters. Since the late 1990s, FVAP has advocated Internet voting as the tool by which the UOCAVA voting problems can be transcended. More recently, its director has espoused FVAP's role as the incubator of Internet voting technology for the nation.[169] Despite the extraordinary growth in the scope and severity of cyber threats to government and private information systems alike during the last decade and the MOVE Act's technical research provisions, FVAP has continued to prioritize development and deployment of Internet voting.

Neither UOCAVA nor MOVE endorsed or required the return of voted ballots in live elections over the public Internet.[170] Nor did these statutes authorize the FVAP to lobby state governments in DoD's name to adopt all-electronic Internet voting technologies. At no point did the agency or DoD publish a legal analysis that assessed whether the voting technology FVAP was funding could satisfy the constitutional requirements for ballots that would be recorded and counted as the voter cast or

HAVA requirements of auditable and accurate voting systems. Nor did the FVAP require the technologies to be tested and certified by the EAC as a prerequisite to receiving funding. The FVAP charted an end run around the entirety of the federal testing and certification apparatus that been developed to assure that votes would be recorded and counted as cast, luring states with financial incentives totaling over $20 million during 2011–12 if they adopted uncertified proto-Internet voting technologies.[171] Given the ease, frequency, and impact of Internet-based fraud and the inability to protect Internet communications from determined remote attackers, FVAP's actions raise considerable legal and pragmatic issues. Arguably, the agency has been engaged in promotion of unlawful voting technologies from at least 2007 forward.

This review of the FVAP's pursuit of Internet voting first provides a high level overview of the complexity of laws and issues thus implicated. It then focuses on FVAP's programmatic plan to achieve Internet voting, followed by a review of Internet voting facts versus the fantasies that have motivated FVAP's director to ridicule the best computer security minds nationally to support his attempt to realize an antiscientific "vision" of internet voting. The final discussion reviews the legal framework for FVAP's power, finding that it has failed to adhere to the congressional revision of FVAP's duties in its pursuit and justification for Internet voting development.

FEDERAL LEGISLATION: UOCAVA, MOVE, AND DEFENSE AUTHORIZATION ACTS

Broad-based federal legislative efforts to assist voting by military and overseas civilian Americans began in 1986 with passage of UOCAVA.[172] In 2002, Congress supplemented UOCAVA's more modest approaches with new provisions in the Help America Vote Act.[173] HAVA authorized the DoD to advise states on legislative changes to their election laws that would enhance UOCAVA voting. The section also mandated periodic state governors' reports to DoD on their states' responses to DoD's recommendations.[174] HAVA also re-codified some provisions from the 2002 National Defense Authorization Act (NDAA), including the directive for the Department to conduct an Internet voting demonstration "pilot" in the 2004 general federal election.[175]

With overseas voting rates considerably lower than domestic voting rates, two nonprofit think tanks and the EAC conducted studies to identify the most significant impediments UOCAVA voters have faced in casting ballots.[176] They learned that the transmission time through the domestic, foreign, and military mail systems needed for each required sequential step in the voting process posed the most significant hurdle. Most states had required the absentee voter to register to vote (if not already registered), then request and receive a blank absentee ballot, and finally return the marked ballot all within a narrow specified period before the hard deadline of Election Day. Passage of the MOVE Act[177] in 2009 sought to eliminate this transmission delay by requiring states to offer electronic (over the Internet) options for voter registration, application for absentee ballots, and blank ballot delivery. The

Act also modified time limits for some tasks and mandated a minimum of 45 days of absentee ballot availability prior to Election Day, as the nonprofits recommended.[178]

It is important to note that the MOVE Act did not require states to *substitute* electronic transmissions for more secure but slower traditional postal mail when performing election tasks. Instead, MOVE directed states to supplement their traditional processes by offering UOCAVA voters a choice of using the electronic, Internet-based method for the steps leading up to but not including the marking and return of a voted ballot.[179] Thus, the MOVE Act pointedly drew a line between preliminaries to voting and the act of marking a ballot and returning it for the count. MOVE did not require or encourage states to approve the electronic transmission of *voted* or marked ballots, reflecting the vulnerability of the election system and the individual voter's marked ballot to automated cyber fraud.[180]

From the mid-2000s through part of 2012, FVAP was lobbying states for "all-electronic elections" without distinguishing the security vulnerabilities associated with the transmission of voted or marked ballots from those of blank ballots. During this period, 33 states modified their laws to permit UOCAVA voters to transmit voted ballots over the Internet in some circumstances, with the majority permitting e-mail of voted ballots.[181] The appendix inventories the state law modification of ballot secrecy laws. While all 50 states assure ballot secrecy to their domestic voters, at the FVAP's request, more than half the states now reduce these protections for UOCAVA voters. MOVE is silent on whether local election agencies (or FVAP) must inform overseas voters of the different levels of voting success depending on the type of balloting method. But no legal impediment bars states from providing cyber security disclosures to voters so they can select the method best able to protect their votes from hacking or other covert modifications.

Although the MOVE Act's mandates improved UOCAVA voters' ability to cast timely ballots, the new requirements dramatically increased the technological and security demands on states and localities.[182] The Act's passage in late December 2009 required states to provide substantial new services during the 2010 federal election cycle that had already commenced.[183] Many states had less than six months to study technical options; obtain budget approval; and procure, test, and deploy the newly required capacity for specified Internet-facing voting services even though they excluded voted ballot transfer. Moreover the jurisdictions needed to acquire sufficient staff or capability to assure their secure and reliable operation.[184] With enactment occurring in the midst of a major election cycle, election officials often lacked the budgets, the staff expertise, and the time to implement MOVE fully. Compounding the problems, MOVE's short implementation period placed officials at the mercy of vendors who overstated the qualities of their products to assure the fast sale. The constricted time did not permit officials to undertake careful and comparative assessments in the public interest or to negotiate contracts with appropriate protections for the public interest.

Two election policy trends can be discerned from the three federal enactments—UOCAVA, HAVA, and the MOVE Act—that address voting technology.[185]

First, they significantly increased the federalization of absentee ballot procedures, culminating in the MOVE Act's implied pre-emption of conflicting state election laws. Second, the laws imposed new federal mandates for deployment of computer and network technologies to aid UOCAVA voters (short of voted ballot delivery), reflecting high confidence in these systems' capacity to supply reliable, secure information transmissions. Unfortunately, because these Internet-connected voting technologies have not been developed with high assurance techniques designed to achieve superior levels of data accuracy and system and data security, their performance will be marred by software bugs and the ubiquitous internet threats; these range from hacking to malware to system unavailability because of concerted attacks to take down the site.[186] The FVAP has proceeded forward anyway, including into the funding of mobile phone voting—possibly the single most vulnerable voting device yet constructed and subject to spyware.[187] The agency's technical hubris is sadly misplaced, for it did not delay its activities until the public Internet and the software on PCs and mobile devices can be re-architected and re-engineered for high security.[188]

The two federal mandates that concentrate federal policy power over absentee ballots apply not only to overseas voters but also to military personnel located in the United States. Once adopted, these new technical systems can "bleed over," leading to rapid changes in state and local election practices for domestic voters. New technologies and managerial systems have previously been introduced to serve a particular subset of voters, but fiscal and administrative pressures almost invariably arise to unify voting and administrative support systems. Thus, technological changes initially adopted for UOCAVA voters may—and often have—become generalized to the whole. Where, as here, the new mandates have been interpreted to require deployment of Internet-connected electronic technologies in "mission-critical"[189] areas of election administration, the new security threats[190] can endanger the integrity and legitimacy of the entire election and not only UOCAVA ballots.

In the MOVE Act's wake but apparently under the radar of busy DoD security experts and DoD attorneys, beginning in 2007 FVAP applied even greater pressure on the states to move to all-electronic elections while trading on DoD's reputation for expertise in cyber security.[191] FVAP's leadership and its direct supervisors in the Division of Personnel and Readiness lack computer security expertise and election law knowledge. Not surprisingly, they have not reined in the agency from its "don't worry, be happy" cheerleading approach to sponsoring unproven innovation in election technologies that risk substantial disenfranchisement and illegitimate electoral results. As a result, many state governments are now deploying FVAP-funded online ballot marking systems that send marked ballots over the Internet (from the vendor's software to the voter's computer) that cannot provide ballot privacy or other essential protections.[192] The FVAP continues to equivocate in its terminology, failing to acknowledge the security differences between blank and voted ballot transmissions.[193] FVAP's failure to disclose and warn of the differential security properties of these two types of ballots has contributed to lawyers and election officials not discerning the congressional line that excluded voted ballots from MOVE's mandate of electronic support for election activities.[194]

Where a state or the FVAP justifies an Internet voting option only for UOCAVA voters, the inequality in convenience will also lead to pressures to expand the service option to all voters. The states will also want to accrue maximum return from the hardware and software investments made to support UOCAVA voters. Federal policymakers, including those at the FVAP/DoD, have not demonstrated awareness of these state and local election infrastructural facts,[195] or the continuing costs of defense-in-depth security for Internet-facing election technologies.[196] With FVAP positioned inside DoD, security assessments are unlikely to transpire in the state, for they are unlikely to understand that DoD has not validated the quality or security of these voting systems. The voting systems vendors' capture of the DoD funding and deployment apparatus agency could lead to an insulation of their products from any meaningful scrutiny. With proper legal supervision within DoD and in the states, the fundamental right to vote and the correlative right to have votes accurately recorded and cast will lead to the close scrutiny of any voting system deployed in federal elections. But this task has yet to be shouldered.

THE FVAP'S CHEERLEADING FOR INTERNET VOTING

In the late 1990s and early 2000s, the FVAP identified its set of preferred solutions to increase UOCAVA voters' participation rates, producing several documents favoring all-electronic voting technologies.[197] During the late 1990s adoption of digital information systems and networked communications were widely viewed as presenting opportunities for greatly increased efficiency with very little downside risk. In 1998, the agency conducted its first Internet-based election with actual voted ballots. Thus, FVAP formulated its vision of Internet voting as the ideal voting method for highly mobile or distant citizens prior to the September 11, 2001 attacks, and prior to the current legislative understanding that Internet-facing networked information systems offer large new attack surfaces that present significant national security risks. FVAP also became committed to Internet voting before the available data showing UOCAVA voters have extremely low rates of voter registration as compared with domestic voters.

Despite the dangers posed by Internet voting, and undoubtedly in a good faith effort to expand overseas voters' electoral participation, the FVAP has encouraged transmission of marked (voted) ballots over the public Internet.[198] FVAP has represented to state governments in legislative hearings and in letters to state governors or secretaries of state (the chief election officers) that achieving all-electronic elections over the Internet is a U.S. Department of Defense policy goal for supporting overseas voters.[199]

INTERNET VOTING: SEPARATING LEGALLY RELEVANT FACTS FROM FANTASY

Having the option of casting marked ballots online appears to offer advantages that include maximum convenience, broad access,[200] and the eventual possibility of lowered costs through elimination of precinct voting and voting machines. Many reality television show contests, such as *American Idol*,[201] use online and telephone voting to generate broad audience participation. Non-governmental organizations, such as alumni boards and labor unions, often conduct online elections.[202] Financial institutions and merchants have increasingly nudged their customers to transact their banking business and shopping over the Internet.[203] Thus, it is a common misunderstanding that no sound reasons remain for not moving governmental voting, or at least UOCAVA voting, to the Internet. Neither lawyers nor members of the general public are trained in threat modeling for cyber security. They may not understand that the relative value of attacks on an alumni board-elect versus United States elections are vastly different.

Our election law is premised upon a constitutional commitment to popular sovereignty as expressed through democratic processes for selecting a representative government.[204] Realizing these fundamental principles implies—or perhaps necessitates—voters' capacity to cast ballots free from coercion and that the voting system and its human administrators correctly determine and report the authentic winners of the election as defined by law. The Supreme Court has repeatedly emphasized that the fundamental right to vote encompasses the integral steps, the right to have the vote correctly counted as cast.[205]

Voters expect—and election statutes generally prescribe—at least four properties of voting system performance that Internet systems cannot reliably achieve: high performance reliability,[206] protection of voter privacy or "ballot secrecy," security of cast ballots and vote tabulations from fraudulent tampering, and the system's proven accuracy in its tallies.[207]

Ballot secrecy is particularly vulnerable in Internet transmissions of voted ballots but is often misunderstood. The scientific and engineering facts of Internet communications establish the inability to assure consistently accurate transmissions of sensitive information in a manner that assures privacy. Regardless of whether a ballot is cast through a web portal or by e-mail, Internet transmissions move from router to router, with forwarding agents passing along the messages through an engineering infrastructure that is owned and managed by corporations, universities, and governmental entities. Third-party re-transmission locations (such as ISPs) function similarly to the old telegraph stations. E-mailed voted ballots permit many ISP and other forwarding agents' employees access to read message contents. As computer scientist David Jefferson notes, "this intrusion [into e-mail messages] does not require sophisticated technical abilities or equipment, but only an ordinary e-mail program that allows viewing of messages and attachments."[208] E-mail forgery (including phishing attacks), identity theft, and fraudulent business transactions are now major categories of criminal fraud. Since most commercial, business, and citizen e-mail is not encrypted, ordinary IT personnel anywhere along the path from sender to receiver may not only read messages, but also filter or modify them—including e-mailed ballots addressed to election offices. Interception and modification of electronic ballots could be easily automated and would be essentially undetectable by the voter and election officials. Importantly, not only the individual UOCAVA voters' rights to a secret and secure ballot are at stake in whether to authorize Internet-return of voted ballots. The systemic integrity of the election and its results are dependent upon ensuring that fraudulent ballots are excluded from the count and that all valid ballots are reflected in the tabulation as originally marked by the voter (voter-cast).

An election could be remotely controlled by yet another technique: a direct attack on the computer server that receives the electronic ballots. As Jefferson observes,

> with Internet voting, virtually any reasonably competent and determined hacker (or government or crime syndicate) anywhere in the world can successfully attack the election server. Competent server attacks, such as that on the Board of Elections and Ethics of Washington DC, perpetrated remotely from the University of Michigan during a public test in October 2010, can take complete control of the server and its voted ballots, and quite possibly without detection.[209]

The Michigan researchers were able to exchange all voters' ballots for phony ballots, and also inserted code directing the server to modify all subsequent ballots received after the attack.[210] Given that the White House, the Federal Bureau of Investigation, and virtually all high technology companies with significant security expertise, staffing, and ongoing investment have been successfully attacked remotely over the Internet,[211] it is unrealistic to predicate voting choices upon the specious proposition that election offices' servers and their voted ballots can be protected from remote attacks.

But a motivated attacker need not attack the server directly to control the election outcomes. Jefferson states that hundreds of potentially successful additional attack methods could be mounted. One particularly devastating version would use the voter's ballot document as the vehicle for inserting malware into the election servers and network. The malware could engender a crash, preventing further receipt of or access to the voted ballots collected, or could insert a virus that modifies ballot choices. Defensive measures for attempting to protect against electoral cyber attack are costly and would greatly increase operational complexity and the needed IT skill set. But even these investments would be insufficient. As MIT computer scientist Ron Rivest has cautioned, "The risks of 'internet voting' more than negate any possible benefits from an increase in franchise. . . . Large institutions [—e.g.,] banks, Google—are successfully attacked all the time. They have much better staff and budgets [than election offices.]"[212] Especially during fiscally challenging times, these costs would render the protective steps highly unlikely.

Malware that secretly resides on millions of voters' personal computers and handheld devices presents yet another vector for election subversion. Jefferson observes that automated malware by international criminal hackers or partisan political operatives "can infect thousands of voters' computers and modify their votes invisibly as they are being transmitted. Again, having a 'secure' connection to the remote election server will make no difference at all. There is no effective way to prevent such an attack, and no effective recovery."[213] The malware could follow the highly successful Zeus format, which is blamed for several hundred million dollars in financial account losses internationally.[214] After Zeus spies on the customer and records the customer's credentials, it fraudulently uses those credentials to transfer funds to an account under criminal control. Voting electronic ballots from personal computers and smart phones could similarly mimic the authentic voter's ballot but actually be an undetectable automatic malware subterfuge whereby the criminal selects the ballot choices and then casts the ballot. Just as vast millions in automated electronic theft were unpreventable and undetected at the time of the Zeus exploits, election theft could be similarly achieved. Hostile foreign adversaries as well as unethical U.S. hackers could covertly deprive American voters of their constitutional rights to self-determination through the ballot box if Internet voting were permitted.[215]

Internet return of voted ballots thus opens wide the doors to modification of cast ballots in undetectable ways, and to interception and blockage of voted ballots so that they cannot reach the election offices for tabulation in a timely manner. E-ballots' capacity to be transmitters of viruses and malware also directly impacts the accuracy and reliability of the recipient jurisdiction's server-computers.

The ABA has underscored the lack of e-mail communications' confidentiality by issuing an ethics opinion that enunciates a professional obligation to warn the client about the risks to confidentiality of sending or receiving electronic communications.[216] One area of particular ABA concern lies in transmitting communications across an employer's network to reach the Internet. Many employers maintain privacy policies specifying that they do not assure privacy on communications over their networks, and they assert a legal obligation to supervise communications sufficiently to assure that laws are not transgressed. Internet-cast ballots over employer networks or devices can produce third-party access to the ballot choices, and also the capability for modifying unencrypted ballots. Yet voting system vendors have not disclosed these risks to ballot privacy and security to their election customers, and in turn, election officials have not warned voters.

Vendors often claim strong security, touting their use of encryption as if it supplies complete protection against all security vulnerabilities. Encryption, however, cannot suffice as a prophylactic against invasion of privacy or disruption of voting.[217] Similar to protective packaging, encryption tools are of widely varying strengths and quality. Proper use requires correct performance of a series of complex procedural steps to generate, secure, and distribute the encryption keys as well as applying an appropriate encryption algorithm.[218] Even if encryption is correctly implemented, that encryption may still eventually be penetrated. Cryptologists assume that given sufficient time, all encryption methods known currently will be broken by methods yet to be discovered, likely as soon as the next decade. [219] Electronic databases containing voted ballots could then reveal voters' choices years after the ballots were cast. This long-term individualized evidence of ballot selections within a vendor's proprietary software remains one of the gravest worries about electronic voting, and especially Internet voting.

Even assuming the ballot encryption was implemented properly and third-party personnel were blocked from reading and modifying a voter's ballot choices, motivated personnel could still intercept and prevent delivery of ballots to the election office. Such interception, which could include essentially throwing away the voted ballots, would be extremely difficult to detect as long as some ballots were delivered; election officials might credibly believe that it was simply a "low turnout" election.[220]

Some election functions that do not include voted ballot transmission are being conducted over the Internet. These include electronic voter registration and blank ballot transfer. MOVE mandates these electronic options for UOCAVA voters.[221] These Internet voting tasks also present significant security threats and technological challenges for assuring that valid registrations reach the election offices and that valid, unmodified blank ballots reach the overseas voter. However, with dedicated attention and sufficient lead-time, the computer security scientists believe the risks to be manageable for the relatively small set of overseas voters. Unfortunately, the MOVE Act mandated the electronic options like blank ballot delivery before the technical answers had been hypothesized, built, and tested. States are struggling with implementation, using uncertified software products. By contrast, MOVE did not authorize the return of voted ballots over the public Internet, nor did it require states to offer voted ballot transmissions to UOCAVA voters.

Given current Internet architecture, engineering, and software quality, the preeminent computer security experts stress the current inability to secure this electronic voted ballot cargo from malware, targeted cyber attacks, and interception and surreptitious modification of cast (marked) ballots. Simply put, the election outcomes can be easily changed, often without detection and without traceability. In close elections with Internet-transmitted ballots, the election officials will undoubtedly be faced with the question of proving a negative: demonstrating that the electronic ballots or their computer servers have not been remotely penetrated. This proof will often not be available without great expense. If the number of Internet ballots is larger than the margin of victory, the impact on voters, on electoral confidence, and on confidence in government could be severely shaken by the serious questions of electoral legitimacy. Thus, understanding the Internet's current engineering and profound security deficits, as well as the security issues pertaining to the PCs and smartphones voters would use, render FVAP's and the vendors' clamor for Internet voting at least a decade premature.[222]

Fortunately, the Military Postal Service Agency expedited its implementation of the MOVE Act in 2010, producing statistical evidence that demonstrates that the timing problems that Internet transmission of voted ballots was originally intended to solve have been virtually eliminated by other strategies sponsored by the MOVE Act.[223] Congress plainly drew some of the most effective initiatives from the Overseas Vote Foundation,[224] including the use of expedited mailing services for absentee ballots. Because some states had not fully implemented the MOVE Act and others received waivers from the duty of full implementation in 2010, the 2010 data will not fully reveal MOVE's impact on UOCAVA rates of valid versus invalid (delayed) ballots.

FVAP'S LEGALLY PROBLEMATIC PROMOTION OF INTERNET VOTING

FVAP's powers and duties have been delineated by statute as well as by administrative directive. Since issuance of DoD Directive 1000.04 in 2004 and continuing into 2011, FVAP has engaged in some significant activities to lay the policy groundwork for transmitting voted ballots over the Internet. These initiatives arguably contradict the Directive's explicit instructions, impairing core election values and arguably undermining systemic election security.[225] The particular efforts FVAP has undertaken are to encourage states to relax ballot secrecy and security requirements for UOCAVA voting, thus permitting electronic transmission of voted ballots.[226] FVAP also has devoted significant time to preliminaries for conducting an Internet voting demonstration program, construing ambiguous decade-old federal legislation as imposing a congressional mandate for it to conduct an Internet voting pilot program in a presidential election.

This section reviews Directive 1000.04 and also considers whether a statutory duty to conduct an Internet voting pilot persists after the MOVE Act's passage. It finds that MOVE extinguished the last legislative basis, arguably imposing on DoD a continuing duty to conduct an Internet voting pilot study. MOVE instead reposes in the DoD's discretion as to whether and what types of voting technology studies shall be conducted for UOCAVA voters' benefit. Consequently, FVAP lacks a statutory mandate for pursuing the Internet voting pilot Congress originally specified in 2002. DoD's capable lawyers could clarify the MOVE Act's withdrawal of the prior mandates. But DoD Secretary Panetta could act to safeguard the nation and UOCAVA votes by eliminating all technology development and requiring FVAP to focus on voter registration.

Election Technology R&D Delegations and DoD Directive 1000.04. Mesmerized by the Internet's apparent promise, in the late 1990s FVAP determined that UOCAVA voters would be best supported by moving to all-electronic elections over the public Internet. FVAP conducted its first Internet voting pilot program in a real election in 1998. The 2002 National Defense Authorization Act (NDAA) then directed DoD to conduct an Internet voting demonstration pilot for military voters in the next presidential election.[227] The NDAA essentially directed that the pilot project eventually named SERVE[228] be conducted in the 2004 presidential election using actual ballots cast by enlisted personnel; Congress did not mandate any pre-deployment technical testing and proof requirements prior to the general election deployment.

Prior to SERVE's implementation, four computer science and security experts on the FVAP-DoD advisory panel publicly released a report that inventoried the breadth of ways the votes cast could be modified surreptitiously.[229] They also addressed the impact on the federal election's legitimacy by introducing opportunities for thousands of fraudulent votes potentially generated by the nation's foreign adversaries. They concluded,

> [b]ecause the danger of successful, large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE immediately and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear.[230]

Following the SERVE Report's publication, in mid-2004, DoD Deputy Secretary Wolfowitz canceled the SERVE project and issued Directive 1000.04 that continues to govern DoD voter assistance activities. The Directive requires FVAP to conduct all of its activities "in a manner *that safeguards the integrity of the electoral process* and *secrecy of the ballot*," and further, "*shall take all necessary steps to prevent fraud and to protect voters against any coercion. . . .*"[231]

The legal principles stated in DoD Directive 1000.04, specifically Sections 4.3.3 and 4.4, enjoy respect and strong support from the voting rights and election security-integrity communities. The historical record is clear that without ballot secrecy/voter privacy, free elections cannot occur; hidden coercion can flourish and fraud can easily occur. Election law treats ballot secrecy not simply as a protection for individual voters' unencumbered capacity to express their political choices, but as a systemic protection of election legitimacy and constitutional popular sovereignty. Unfortunately, FVAP apparently lacked a deep appreciation for the systemic purposes behind ballot secrecy, for it has actively lobbied state and federal supervisory offices to eliminate privacy protection for UOCAVA voters' ballots.[232] Because the principle is listed in Directive 1000.04 as a foundation for DoD's voting activities, FVAP's state legislative lobbying activities in opposition to ballot secrecy are at least curious if not unlawful.

Voting system security experts urge that no voting option should be extended to American military and overseas civilians unless it offers scientifically tested and proven confidence that their ballots will be received and tabulated consistent with their voter-determined ballot markings.[233] Anything less would degrade these Americans' ballots, which would impact systemic interests as well as individual rights. FVAP has repeatedly pressed the Internet voting objective on state governments, however, producing contradictory federal positions on core cyber security policies. In addition to logical inconsistency with protecting the fundamental right to vote, federal advocacy of insecure election practices inherently confuses the state and local governments, which must shoulder the legal duties and implementation burdens.

FVAP continued its approach to pursuing its commitment to an all-electronic elections mission irrespective of both the DoD Directive 1000.4 and computer security science into the first half of 2011. For instance, in March 2011, FVAP submitted its strategic plan for implementing the MOVE Act to Congress and the president. This report pervasively stresses the FVAP's commitment to all-electronic elections. As an example, it states,

> FVAP also proposes the expanded use of email and online transmission for *all election materials throughout the entire UOCAVA absentee voting process*, replacing fax and postal mail where possible. . . . [*T*]*he decision to send a voted ballot by unsecured electronic means must rest with the individual voter based on the voter's desire* to cast his or her vote electronically or to ensure the secrecy of the ballot.[234]

Similar statements of this FVAP policy appear in numerous other documents published over the last five years, despite their noncompliance with DoD Directive 1000.4.[235] While Section 4.3.3 specifically requires all UOCAVA voters to receive DoD/FVAP "voting assistance in a *manner that safeguards the integrity of the electoral process and secrecy of the ballot*," this plan does not explain how FVAP will comply with DoD governing policy protecting ballot secrecy. The Directive recognizes that ballot secrecy is a constituent protection of election legitimacy. The protection is mandated by most states' election laws as well as the DoD Directive.[236] The Directive does not permit individuals to waive their rights to a secret ballot, nor for the FVAP to promote technological voting methods that would necessitate the voter to give up these secret ballot rights. Inexplicably, FVAP neglects the Directive and its critical systemic objectives.

The Directive's Section 4.4 additionally directs all persons who assist in the voting process to "*take all necessary steps to prevent fraud.*" The FVAP's policy stance quoted above misconceives the concerns and scope of systemic protections found in federal election law. It also ignores the counsel of preeminent security experts who advised FVAP officials on the magnitude of Internet-based risks that cannot be effectively mitigated owing to Internet architecture, and their ultimate consequences for enabling undetectable, fraudulent elections.[237] In so doing, the FVAP's lobbying of states for all-electronic elections undermines our national capacity to achieve election cyber security.

The second recent reaffirmation of FVAP's promotion of all-electronic elections and disregard of Directive 1000.04 occurred in May 2011. FVAP issued a solicitation for grant applications that proposed technically "innovative" ways to achieve electronic absentee voting.[238] FVAP drafted its initial funding solicitations for over $20 million to fund proto-Internet voting election technologies with little attention to security and bereft of requirements that the grantees and the projects comply with the foundational election principles enunciated in the DoD Directive.

This FVAP grant program was designed to induce state election offices to purchase election software from voting system vendors, many of which have a history of misrepresenting the security and reliability features of their other e-voting products. These vendors have a regrettably deficient record in achieving system security, Internet security, (election) data integrity, (voter ballot) privacy and secrecy, and other essential objectives.[239] Over $30 million has been allocated in DoD grant funding, with the vast proportion going to Internet voting vendors. The FVAP's technology program is directed by the former executive director of the voting system vendors' trade council, arguably a revolving door that includes conflicts and ethics issues.[240] It also raises questions about "agency capture" by the voting system industry, which has been the beneficiary of well over $20 million in new federal funds without FVAP requiring it to comply with the EAC's voting systems guidelines, HAVA's Title III standards, and the independent testing laboratories certified by the NIST.

Is Congress Requiring an Internet Voting Pilot? Before the 2000s, when the Internet became known as the fastest growing conduit for unprecedented grand larceny, business espionage, and grave national security threats, the Internet was widely viewed to be an unqualified public good whose capabilities could be tapped for quick, relatively cheap communications. Since DoD had funded its creation originally for military purposes, Department executives viewed the benefits of military voting opportunities over the Internet to far outweigh the risks. But the decade of experience with increasingly virulent malware, the persistent inability of national security agencies and the Defense Department to secure their supposed "secured networks" from remote attackers, and the computer scientists' incisive report on intractable Internet voting risks after the first FVAP Internet voting pilot all reduced DoD's enthusiasm for

Internet voting. FVAP leadership somehow discounted the relevance of these points, because well into 2011 it continued its aggressive pressure for realizing the legally superseded prescription for conducting an Internet voting demonstration pilot.

FVAP bases its zealous pursuit of developing an Internet voting pilot on conflicting provisions found in National Defense Authorization Acts (NDAAs) passed from 2000 to 2009.[241] Construing multiple contradictory enactments that address the same subject can lead to a lengthy (and tedious) examination. Thus, this chapter summarizes relevant legislation before briefly identifying two main reasons for construing the last NDAA, which contained the MOVE Act, as the most authoritative.

While primarily focusing on the needs of U.S. troops in foreign conflicts, Congress included several short provisions addressing the desire for the DoD to conduct Internet voting experiments. The 2002 NDAA (enacted in 2001) directed DoD to conduct an "electronic voting demonstration project" in the 2002 federal election.[242] The provision's language also reflects the prevailing conception of risk and technical difficulty presented. Congress authorized the Internet voting demonstration project for an election only a few months hence; it did not specify that any pre-tests be conducted. The statutory language suggests that it expected this to be a no-brainer, successful low threshold-testing outcome. Indeed, FVAP had already conducted what it believed to be a successful Internet voting test in the 2000 presidential election, with 91 total ballots cast. Only in Section 1604(a)(2) does a cautionary note enter; computer and network security and the software development process evidently were not a central part of Congress' time and security calculus. The NDAA also conferred on DoD some limited discretion, permitting the demonstration project to occur in 2004 if national security would be impaired in 2002.[243]

Before the 2004 Internet voting pilot could be conducted, the SERVE Report intervened.[244] Co-authored by four prominent computer scientists and the focus of a lead *New York Times* editorial that counseled the project be terminated consistent with the Report's recommendations, the Report stands as the most comprehensive threat and security assessment yet written of a proposed U.S. Internet voting system. Deputy Secretary of Defense Wolfowitz canceled the pilot project scheduled for the 2004 general election and also issued DoD Directive 1000.04.

The subsequent 2005 NDAA notes the SERVE project's security issues and commences a different path. After restating the direction for an Internet voting pilot, it comments,

> the Secretary may delay the implementation of such demonstration project until the Election Assistance Commission . . . has established electronic absentee voting guidelines and certifies that it will assist the Secretary.[245]

The Conference Report accompanying the bill notes disharmony among the two Houses of Congress but references a compromise, specifically to delay the pilot project.[246] Notably, the Conference Report did not describe the "electronic voting" system it contemplated as requiring every aspect of the voting process to be conducted digitally. The FVAP Director, however, claims that Congress intended that "every aspect" must be electronic and excludes all paper records.[247]

Both the FVAP Director, Robert Carey, and FVAP staff have commented that congressional oversight committee staff have instructed them on Congress's animating intent and expectation in enacting the 2005 pilot project provision. The FVAP Director has underscored these comments as if their content is entitled to great weight in interpreting the legislative language. The implications of these statements, though, are not reflected in the statutory text; there is no evidence that they represent the views of Congress rather than of individual staffers, and they occurred several years after the date of the legislation's passage, when they are no longer part of the congressional process of debate and rebuttal.[248]

Director Carey stresses two documents that issued in 2007 as strong support for his claim of a congressional "mandate" to develop an Internet voting pilot. He points to the 2007 NDAA, which directs, "the Secretary of Defense shall [report] to the Congress . . . in *detail plans for expanding the use of electronic voting technology* for individuals covered under the [UOCAVA]."[249] Yet again, however, the direction lacks content that specifies either an "all-electronic" approach or a "mandate" for FVAP to develop voting technology that uses Internet transmissions of voted ballots. The 2007 NDAA merely requires development of a plan. Such a plan could delineate, consistent with the DoD Directive 1000.04, use of electronic voting in a manner that preserves ballot secrecy and election security. The NDAA's direction could be fulfilled by submitting a plan that largely mirrors later 2009 MOVE Act technology provisions, which omit both a mandates as well as any option to return voted ballots over the Internet.

Carey also has stressed the importance of a Government Accountability Office (GAO) report that describes methods of advancing UOCAVA voting through technology. Carey's emphasis is misplaced, however, because the GAO used a military personnel and readiness expert who lacked both computer security and election law expertise yet detailed him to provide voting technology recommendations. This personnel officer's cheerleading recommendation fails miserably in its understanding of the Internet's security attributes and possibilities. He concludes:

> [DoD should c]reate an *integrated, comprehensive, long-term, results-oriented plan for future electronic voting programs* that specifies . . . the goals to be achieved along with tasks including identifying safeguards for the security and privacy of all DOD's voting *systems—both electronic and Internet.*
>
> - The plan should also *specify milestones, time frames, and contingencies*;
> - *Synchronize them with planned development of the Commission's guidelines for Internet voting*;
>
> [The GAO shall report to] Congress . . . the assessment of . . . the *progress of [DoD] and the [EAC] in developing a secure, deployable system for Internet-based electronic voting* pursuant to [the 2005 NDAA].[250]

Exhortations to adopt Internet voting from those lacking computer science and security gravitas embody the "oxy-topian" approach to voting systems. Preeminent MIT computer security expert Ron Rivest has observed:

> [t]he obvious "solution" for the future would be a remote voting system where everyone can vote over the Internet in an auditable manner, and where vote-selling and voter coercion are altogether prevented.
>
> *Let me call this the "oxy-topian" voting system.* Here "oxytopian" is a combination of the two words "oxymoron"—self-contradictory—and "utopian"—ideal, because such a set of "ideal" requirements is intrinsically oxymoronic and unrealizable.[251]

The defense personnel expert whom the GAO permitted to file this report obviously did not understand technical limitations and contradictions within his recommendation. Unfortunately, because this report issued from the respected GAO, though not from its experts in computer security, it may have misled Congress and the FVAP on the prospects for developing "secure Internet voting."

Congress passed the most recent legislation, the MOVE Act, as a component of the 2010 NDAA. MOVE requires states to offer electronic Internet-based options for voting tasks preceding, but excludes options for Internet-marking of the ballot and its return.[252] In Section 589 of the Act, Congress delegated to the Secretary of DoD the discretion of choosing whether to develop additional technological options for UOCAVA voters. This comprehensive congressional delegation of discretion concerning all UOCAVA technical voting research, within a larger, comprehensive act that redressed UOCAVA deficiencies, entitles the MOVE Act to special weight when attempting to construe the earlier NDAA provisions' survival as potentially mandating an Internet voting pilot project.[253] Adding additional weight to this construction, Section 589 also re-codifies parts of the earlier NDAAs concerning the roles of EAC and NIST in developing Internet voting white papers and standards, but pointedly did not re-codify the direction to DoD to conduct an Internet voting pilot. This omission should be construed as congressional withdrawal of the prior pilot-development directives.

Instead of the earlier NDAA directions surviving independently of MOVE, the MOVE Act taken as a whole and Section 589 read carefully show that Congress had developed greater awareness of the cyber security threat. The MOVE legislation also requires preservation of Directive 1000.04, which incorporates protections that block the ability to conduct Internet voting.[254] Congress chose to codify completion of the earlier-mandated agency studies and issuance of guidelines, but did not repeat or recodify the direction or "mandate" to conduct a live-election Internet voting test with real ballots. Recognizing the sensitivity of the voting process and the larger cyber security threat, Congress deferred the question of whether and how to structure an Internet voting pilot to the Secretary. Thus, Congress implicitly and selectively incorporated parts of the 2002 and 2005 NDAAs but implicitly repealed the 2002 mandate for conducting an Internet voting pilot.

As late as February 2012, FVAP Director Carey continued to profess confidence that Congress's NDAAs compel the agency to conduct an Internet voting pilot.[255] Given Director Carey's announced departure from the DoD in June 2012, the DoD's interpretation of the MOVE Act's impact on the NDAAs may change with the introduction of new leadership. Appearing to fast-track the technical infrastructure for

Internet voting before the cyber security-aware new Secretary of Defense could exercise review, the FVAP has issued at least two multi-million dollar grant solicitations to fund new voting technologies. This grant program included solicitations for at least $20 million that ultimately awarded untested and uncertified proto-Internet voting systems to state governments. These systems arguably violate HAVA's Title III standards for auditability and accuracy as well as Directive 1000.04, but Director Carey rejected the proposition that FVAP owed any duty to ensure that the voting technologies it funded complied with other federal voting system laws.[256]

Given that UOCAVA citizens' voter registration rates are relatively low compared with domestic voters, some have argued FVAP can best solve the UOCAVA voting problem by focusing on augmenting military and overseas civilian voter registration rates. If not a complete solution, registration still constitutes the threshold requirement in order to cast a ballot.[257] Instead of a DoD agency funding insecure election technologies, a more effective effort at solving the military participation issues would focus on creating a culture of voting that begins with enlistment. If FVAP would cease its romantic affair with Internet voting technologies and instead focus on the hard work of building a voting culture that values election participation and security, as well as ballot privacy and fiscal prudence, it would earn more respect and quite possibly better results.

DoD might prudently consider restricting the scope of its voting responsibilities by requesting that it exclusively serve enlisted personnel and their families and be explicitly relieved of all voting technology development activity. FVAP lacks the staffing, security expertise, and other components needed for conducting election technology research and development. Until the technology duties have ended, government efficiencies from leveraged expertise could be achieved if the DoD would contract with NIST and independent academic scientists for any desired election technology research and development. EAC's role as an advisor should be preserved, as it is bipartisan and is required to conduct itself with greater transparency than DoD.

If DoD were to support congressional transfer for overseas civilians' voting participation into the State Department's care, FVAP and DoD would not only streamline their electoral mission and likelihood of success, but also augment the possibility of better governmental service for remote civilian voters. DoD Secretary Panetta has not yet taken a public stand on FVAP and its technology development programs. His leadership is needed to right the FVAP ship. He could require DoD to work with DHS in developing an initiative to help correct FVAP's misrepresentations regarding the capacity for secure Internet voting in the near future, and assist in the American public's development of greater sophistication in cyber security.

Moving Forward

Professionalism norms counsel lawyers to deal with facts as they find them, rather than to indulge in fictions or assumptions that are more preferable. Applying that insight to voting technology requires first that we not trust computer technologies to record and tabulate votes accurately unless a robust quality control system is instituted that can provide independent checks of their accuracy.[258] Post-election auditing or "recounting" using paper ballot records can provide the independent check on the voting machines.[259] Recounting using an extrinsic record independent of the software should be recognized as essential for preserving voting rights and become a routine practice when computer-based voting equipment is deployed.

The past two decades of federal regulatory involvement in voting technology arguably have produced little public benefit, but rather a striking reduction of election security and public accountability. Repeatedly, Congress has allocated voting technical policy responsibilities to those who lack the educational background to understand a digital voting system's "threat assessment" and how the "insider problem"—standard concerns within computer security—relates to assuring voting rights. Both the EAC and the FVAP have persistently been led by persons who seek the public benefit but who lack election law and election technical competence. DOJ's voting section possesses enviable election law expertise but remains bereft of technical capability, though statutory law vests the Department with enforcement of voting system standards. If the federal government seeks to shoulder responsibilities in the voting technology arena, the law should require that the agencies will be structured and led by those who will seek to ensure that scientific facts about computers and their security issues are not treated as simply unwelcome opinions. With sound intercession by the Secretary of Defense and Attorney General, and congressional restructuring of federal election powers, this dangerous trajectory can be corrected.

ACKNOWLEDGMENTS

Scientists, nonprofit advocates, election officials, scholars, and lawyers generously contributed their knowledge to this chapter. Computer scientists Matt Bishop, David Jefferson, Andrew Appel, Alex Halderman, Ron Rivest, Barbara Simons, Doug Jones, Jeremy Epstein, Noel Runyan, Harri Hursti, Peter Neumann, and David Wagner work tirelessly with lawyers and policy makers to illuminate the realistic versus fanciful expectations of computers and software in the voting context. I am deeply in their debt. Statistics and election auditing scholars Philip Stark and Mark Lindeman, plus election officials and nonprofit advocates who seek election transparency and accuracy, greatly assisted with this project. They include Lowell Finley, Doug Kellner, Susannah Goodman, Matt Damschroder, Pam Smith, Ion Sancho, Dan McCrea, Howard Stanislevic, Ellen Theisen, Eric Marshall, Eddie Hailes, Holly Jacobson, Neal McBurnett, Luther Weeks, Susan Greenhalgh, Marc Rotenberg, Lillie Coney, Larry Norden, Jane Platten, Sean Flaherty, and Margit Johansson. Law student research assistants Sarah Kendrig and Nicholas Kopcho, plus Karen Isobe, worked with law librarians Amy Burchfield, Tom Hurray, and Schuyler Cook in providing crucial support, especially in developing the chart of state ballot secrecy laws (appendix). George Taylor and David Jefferson contributed critiques of multiple drafts, for which I am especially appreciative. Policy and legal recommendations, as well as any errors, should be attributed exclusively to the author.

Appendix: Contradictory State Laws Governing Election Fraud and Integrity

State	Permit UOCAVA voters to return ballots electronically? (includes fax, e-mail, and Internet portal)	Permit *all* voters to return voted ballots electronically? (includes fax, e-mail, and Internet portal)	Require ballot secrecy for in-person voting?
Alabama	No	No, mail or in-person only	Yes: Ala. Code § 17-6-34; voters are allowed to have assistance, § 17-9-13
Alaska[a]	Yes, fax only	Yes, fax only	Yes: Alaska Stat. § 15.15.060; exceptions for disabled persons who need assistance, § 15.15.240
Arizona[a]	Yes, fax and Internet Pilot Program	Yes, fax or Arizona's secure ballot upload system	Yes: Ariz. Const. art. 7, § 1; disability exception: Ariz. Rev. Stat. §§ 16-578, 16-580
Arkansas	No	No, mail or in-person only	Yes: Ark. Code Ann. § 7-5-309; disability exception: § 7-5-310, -311
California	Yes, fax only	No, mail or in-person only	Yes: Cal. Elec. Code §§ 14276, 14287, 14293; child care exception: § 14222
Colorado	Yes, e-mail, fax; Internet Pilot Program	No, mail or in-person Only	Yes: Colo. Rev. Stat. Ann. §§ 1-7-304, -503; disability exception: § 1-7-11
Connecticut	No	No, mail or in-person only	Yes: Conn. Const. art. 6, § 5, Conn. Gen. Stat. Ann. § 9-236b; disability exception: Conn. Gen. Stat. Ann. § 9-264
Delaware[a]	Yes, e-mail and fax	No, mail or in-person only	Yes: Del. Const. art. 5, § 1; disability exception: Del. Code Ann. tit. 15, § 4943
District of Columbia	Yes, fax and e-mail	No, mail or in-person only	Yes: D.C. Code § 1-1001.09(a); disability exception: § 1-1001.09(f)
Florida[b]	Yes, fax only	No, mail or in-person only	Yes: Fla. Stat. Ann. § 101.041; disability exception: § 101.051
Georgia	Yes, Internet Pilot Program	No, mail or in-person only	Yes: Ga. Code Ann. § 21-2-70(13); disability exception: § 21-2-385.1
Hawai'i[b]	Yes, fax only	No, mail or in-person only	Yes: Haw. Rev. Stat. § 11-137; disability exception, § 11-139

Notes: Research is current to October 2011.

a = ID required for in-person voting but allows unsecure electronic voting

b = Photo ID required for in-person voting but allows unsecure electronic voting

c = ID required, photo required after DOJ preclearance for in-person voting but allows unsecure electronic voting

Require ballot secrecy for standard, absentee, or mail-in voting?	Require ballot secrecy for UOCAVA voting?	Require polling place voter ID? Photo required?	State
Yes, for mail-in absentee voting: Ala. Code § 17-11-9	Yes, UOCAVA voting same as standard absentee, Ala. Code § 17-11-9	Yes, photo not required	Alabama
Yes, for mail and in-person absentee voting; no, for electronic transmission: Alaska Stat. § 15.20.066	Yes for mail-in absentee, no for electronic transmission, Alaska Stat. § 15.20.066	Yes, photo not required	Alaska
Yes, for mail-in absentee voting: Ariz. Rev. Stat. § 16-548	Yes for mail-in absentee, no for fax, Internet, and FWAB votes by electronic trans (secrecy waiver)[a]	Yes, photo not required	Arizona
Yes, for mail-in absentee voting: Ark. Code Ann. § 7-5-412	Yes, same as standard absentee voting, Ark. Code Ann. § 7-5-412	Yes, photo not required	Arkansas
Yes, for mail-in absentee voting: Cal. Elec. Code § 3017	Yes for mail-in absentee voting, if faxing must include "Oath of Voter" waiving right to confidential vote[a]	No	California
Yes, for mail-in absentee voting: Colo. Rev. Stat. Ann. § 1-8-101	Yes for mail-in absentee and electronic transmission of votes, Colo. Rev. Stat. Ann. § 1-5.5-101	Yes, photo not required	Colorado
Yes, for mail-in absentee voting: Conn. Gen. Stat. Ann. §§ 9-137, -139	Yes, same as standard absentee voting	Yes, photo not required	Connecticut
Yes, for mail-in absentee voting: Del. Code Ann. tit. 15, § 5504	Yes if returning voted ballots by mail, no for electronic transmission: Del. Code Ann. tit. 15, § 5525	Yes, photo not required	Delaware
Yes, for mail-in absentee voting: D.C. Code § 1-1001.09(a)	Yes when returning voted ballots by mail	No	District of Columbia
Yes, for mail-in absentee voting: Fla. Stat. Ann. § 101.6103	Yes for mail-in absentee voting: Fla. Stat. Ann. § 101.6103(7); no for electronic transmission: Fla. Admin. Code r. 1S-2.030(6)(f)	Yes, photo ID required	Florida
Yes, for mail-in absentee voting: Ga. Code Ann. § 21-2-384(b)	Yes for mail-in absentee voting: Ga. Code Ann. § 21-2-384(e); yes for electronic transmission: § 21-2-387(b)(4)	Yes, photo ID required	Georgia
Yes, for mail-in absentee voting: Haw. Rev. Stat. § 15-6	Yes for mail-in absentee voting: Haw. Rev. Stat. § 15-6; no for electronic transmission: § 15-5(2)	Yes, photo ID required	Hawai‘i

State	Permit UOCAVA voters to return ballots electronically? (includes fax, e-mail, and Internet portal)	Permit *all* voters to return voted ballots electronically? (includes fax, e-mail, and Internet portal)	Require ballot secrecy for in-person voting?
Idaho	Yes, e-mail and fax for emergencies	No, mail or in-person only	Yes: Idaho Code Ann. § 34-1107; disability exception: § 34-1108
Illinois	No	No, mail or in-person only	Yes: Ill. Const. art. 3, § 4; disability exception: 10 Ill. Comp. Stat. Ann. 5/17-14
Indiana[b]	Yes, e-mail and fax	No, mail or in-person only	Yes: Ind. Code § 3-11-7.5-8, 3-11-13-8; disability exception: § 3-11-9-2
Iowa	Yes, e-mail and fax: military only in combat zones	No, mail or in-person only	Yes: Iowa Code Ann. § 49.84; disability exception: § 49.90
Kansas[a]	Yes, e-mail and fax	No, mail or in-person only	Yes: Kan. Const. art. 4, § 1; disability exception: Kan. Stat. Ann. § 25-2909
Kentucky	No	No, mail or in-person only	Yes: Ky. Const. § 147; disability exception: Ky. Rev. Stat. § 117.255
Louisiana[b]	Yes, fax only	Yes, fax only	Yes: La. Const. art. 11, § 2; disability exception: La. Rev. Stat. Ann. § 18:106
Maine	Yes, fax only	No, mail or in-person only	Yes: Me. Rev. Stat. Ann. tit. 21-A, § 671(8); disability exception: § 672
Maryland	No	No, mail or in-person only	Yes: Md. Code, Elec. Law, § 9-203; disability exception: § 10-310
Massachusetts	Yes, e-mail and fax	No, mail or in-person only	Yes: Mass. Const. pt. 1, art. 9; disability exception: Mass. Gen. Laws Ann. ch. 54, § 79
Michigan[b]	No	No, mail or in-person only	Yes: Mich. Const. art. 2, § 4; disability exception: Mich. Comp. Laws Ann. § 168.751

Notes: Research is current to October 2011.

a = ID required for in-person voting but allows unsecure electronic voting

b = Photo ID required for in-person voting but allows unsecure electronic voting

c = ID required, photo required after DOJ precleareance for in-person voting but allows unsecure electronic voting

Require ballot secrecy for standard, absentee, or mail-in voting?	Require ballot secrecy for UOCAVA voting?	Require polling place voter ID? Photo required?	State
Yes, for mail-in absentee voting: IDAHO CODE ANN. § 34-1004	Yes for mail-in absentee voting: IDAHO CODE ANN. § 34-1004; undetermined for faxed votes: § 34-201	Yes, photo ID required	Idaho
Yes, for mail-in absentee voting: 10 ILL. COMP. STAT. ANN. 5/19-5	Yes for mail-in absentee voting: 10 ILL. COMP. STAT. ANN. 5/20-5	No	Illinois
Yes, for mail-in absentee voting: IND. CODE § 3-11-10-1	Yes for mail-in absentee voting: IND. CODE § 3-11-10-1; no for electronic transmission: 3-11-10-1(b), 3-11-4-6(h)	Yes, photo ID required	Indiana
Yes, for mail-in absentee voting: IOWA CODE ANN. § 53.17	Yes for mail-in absentee voting: IOWA ADMIN. CODE r. 721-21.320(3); no for electronic transmission: r. 721-21.320(4)(a)	No	Iowa
Yes, for mail-in absentee voting: KAN. STAT. ANN. § 25-1120	Yes for mail-in absentee voting: KAN. STAT. ANN. § 25-1221; no for electronic transmission: § 25-1216	Photo ID required after Jan. 1, 2012	Kansas
Yes, for mail-in absentee voting: KY. REV. STAT. § 117.086	Yes for mail in absentee votes: KY. REV. STAT. § 117.086	Yes, photo not required	Kentucky
Yes, for mail-in absentee voting: LA. REV. STAT. ANN. § 18:1310(A)(1)	No secrecy for UOCAVA voters, even by mail: LA. REV. STAT. ANN. § 18:1310(A)(2)	Yes, photo ID required	Louisiana
Yes, for mail-in absentee voting: ME. REV. STAT. ANN. tit. 21-A, § 754-A	Yes for mail-in absentee voting: ME. REV. STAT. ANN. tit. 21-A, § 782; electronically returned ballots to be handled same as mailed: § 783(5)	No	Maine
Yes, for mail-in absentee voting: MD. CODE, ELEC. LAW § 9-303, 310	No distinction made for military absentee voters	No	Maryland
Yes, for mail-in absentee voting: MASS. GEN. LAWS ANN. ch. 54, § 92	Yes for mail-in absentee voting: MASS. GEN. LAWS ANN. ch. 54, § 87; no for electronic transmission: § 95	No	Massachusetts
Yes, for mail-in absentee voting: MICH. COMP. LAWS ANN. § 168.764a	Yes for mail-in absentee voting: MICH. COMP. LAWS ANN. § 168.764a; no for electronic transmission MICH. COMP. LAWS ANN. §168.759a(8)	Yes, photo ID required	Michigan

State	Permit UOCAVA voters to return ballots electronically? (includes fax, e-mail, and Internet portal)	Permit *all* voters to return voted ballots electronically? (includes fax, e-mail, and Internet portal)	Require ballot secrecy for in-person voting?
Minnesota	No	No, mail or in-person only	Yes: Minn. Stat. Ann. § 204C.18; disability exception: § 204C.15
Mississippi	Yes, e-mail and fax	No, mail or in-person only	Yes: Miss. Code Ann. § 23-15-465; disability exception: § 23-15-549
Missouri[a]	Yes, e-mail and fax in hostile fire areas only	No, mail or in-person only	Yes: Mo. Const. art. 8, § 3; disability exception: Mo. Rev. Stat. § 115.445
Montana[a]	Yes, e-mail and fax	No, mail or in-person only	Yes: Mont. Const. art. 4, § 1; disability exception: Mont. Code Ann. § 13-13-119
Nebraska	Yes, e-mail and fax	No, mail or in-person only	Yes: Neb. Const. art. VI, § 6; disability exception: Neb. Rev. Stat. § 32-918
Nevada	Yes, e-mail and fax	No, mail or in-person only	Yes: Nev. Rev. Stat. § 293.2546; disability exception: § 293.296
New Hampshire	No	No, mail or in-person only	Yes: N.H. Const. pt. 1, art. 11; disability exception: N.H. Rev. Stat. Ann. § 659.20
New Jersey	Yes, e-mail and fax	No, mail or in-person only	Yes: N.J. Stat. Ann. §19:15-26; disability exception: N.J. Stat. Ann. § 19:50-3
New Mexico[a]	Yes, e-mail and fax	No, mail or in-person only	Yes: N.M. Const. art. 7, § 1; disability exception: N.M. Stat. Ann. § 1-12-15 (1978)
New York	No	No, mail or in-person only	Yes: N.Y. Const. art. 2, § 7; disability exception: N.Y. Elec. Code § 8-306

Notes: Research is current to October 2011.

a = ID required for in-person voting but allows unsecure electronic voting

b = Photo ID required for in-person voting but allows unsecure electronic voting

c = ID required, photo required after DOJ preclearance for in-person voting but allows unsecure electronic voting

Require ballot secrecy for standard, absentee, or mail-in voting?	Require ballot secrecy for UOCAVA voting?	Require polling place voter ID? Photo required?	State
Yes, for mail-in absentee voting: Minn. Stat. Ann. § 203B.07	Yes for mail-in absentee voting: Minn. Stat. Ann. § 203B.21; Electronic retun not allowed	No	Minnesota
Yes, for mail-in absentee voting: Miss. Code Ann. § 23-15-631, 633	Yes for mail-in absentee voting: Miss. Code Ann. § 23-15-699(2); electronic transmission security not guaranteed, § 23-15-699(5)	No	Mississippi
Yes, for mail-in absentee voting: Mo. Rev. Stat. § 115.291	Yes for mail-in absentee voting: Mo. Rev. Stat. § 115.291; no mention of secrecy for electronic transmission: 115.291(3), (4)	Yes, photo not required	Missouri
Yes, for mail-in absentee voting: Mont. Code Ann. § 13-13-201	Yes for mail-in absentee voting: Mont. Code Ann. § 13-13-241; no guarantee of electronic transmission secrecy: § 13-21-207	Yes, photo not required	Montana
Yes, for mail-in absentee voting: Neb. Rev. Stat. § 32.947	Yes for mail-in absentee voting: Neb. Rev. Stat. § 39-939.02(6); no mention of secrecy for electronic transmission	No	Nebraska
Yes, for mail-in absentee voting: Nev. Rev. Stat. § 293.325	Yes for mail-in absentee voting: Nev. Rev. Stat. § 293.3157(2); no for electronic transmission: § 293.3157(3)	No	Nevada
Yes, for mail-in absentee voting: N.H. Rev. Stat. Ann. § 657:17	Yes for mail-in absentee voting: N.H. Rev. Stat. Ann. § 657:17; no electronic return of voted materials allowed	No	New Hampshire
Yes, for mail-in absentee voting: N.J. Stat. Ann. § 19:63-16	Yes for mail-in absentee voting: N.J. Stat. Ann. § 19:59-10; no for electronic transmission of voted ballot: § 19:59-14	No	New Jersey
Yes, for mail-in absentee voting: N.M. Stat. Ann. § 1-6-9(A) (1978)	Yes for mail-in absentee voting: N.M. Stat. Ann. § 1-6-9(B) (1978); no for electronic transmission: § 1-6-9(C)	Yes, photo not required	New Mexico
Yes, for mail-in absentee voting: N.Y. Elec. Code § 8-410	Yes for mail-in absentee voting: N.Y. Elec. Code § 10-112; no electronic transmission allowed: § 10-107(2)	No	New York

State	Permit UOCAVA voters to return ballots electronically? (includes fax, e-mail, and Internet portal)	Permit *all* voters to return voted ballots electronically? (includes fax, e-mail, and Internet portal)	Require ballot secrecy for in-person voting?
North Carolina	Yes, e-mail and fax	No, mail or in-person only	Yes: N.C. GEN. STAT. § 163-166.2, art. 6; disability exception: N.C. GEN. STAT. ANN. § 163-166.8
North Dakota[a]	Yes, e-mail and fax	No, mail or in-person only	Yes: N.D. CONST. art. 2, § 1; disability exception: N.D. CENT. CODE § 16.1-13-27
Ohio	No	No, mail or in-person only	Yes: OHIO REV. CODE § 3599.20; disability exception: § 3505.24
Oklahoma[a]	Yes, fax only	No, mail or in-person only	Yes: OKLA. STAT. ANN. tit. 12, § 2507; disability exception: OKLA. STAT. ANN. tit. 26, § 7-123.3
Oregon	Yes, fax only	No, mail or in-person only	Yes: OR. REV. STAT. § 254.472; disability exception: § 254.445
Pennsylvania	No	No, mail or in-person only	Yes: PA. CONST. art. 7, § 4; disability exception: 25 PA. STAT. ANN. § 3058
Rhode Island	Yes, fax only	No, mail or in-person only	Yes: R.I. GEN. LAWS § 17-19-24; disability exception: § 17-19-26.1
South Carolina[c]	Yes, e-mail and fax	No, mail or in-person only	Yes: S.C. CONST. art. 2, § 1; disability exception: S.C. CODE § 7-13-770
South Dakota	No	No, mail or in-person only	Yes: S.D. CONST. art. 7, § 3; disability exception: S.D. CODIFIED LAWS § 12-18-25
Tennessee	Yes, fax only	No, mail or in-person only	Yes: TENN. CODE ANN. § 2-7-103; disability exception: § 2-7-116

Notes: Research is current to October 2011.

a = ID required for in-person voting but allows unsecure electronic voting

b = Photo ID required for in-person voting but allows unsecure electronic voting

c = ID required, photo required after DOJ preclearance for in-person voting but allows unsecure electronic voting

Require ballot secrecy for standard, absentee, or mail-in voting?	Require ballot secrecy for UOCAVA voting?	Require polling place voter ID? Photo required?	State
Yes, for mail-in absentee voting: N.C. Gen. Stat. Ann. § 163-231	Yes for mail-in absentee voting: N.C. Gen. Stat. Ann. § 163-250; no mention of secrecy for electronic transmission: § 163-257	No	North Carolina
Yes, for mail-in absentee voting: N.D. Cent. Code § 16.1-07-11	Yes for mail-in absentee voting: N.D. Cent. Code § 16.1-07-11; no specific secrecy guidelines for electronic return of voted ballots: § 16.1-07-05(2)	Yes, photo not required	North Dakota
Yes, for mail-in absentee voting: Ohio Rev. Code § 3509.05	Yes for mail-in absentee voting: Ohio Rev. Code § 3511.09; no electronic transmission permitted	Yes, photo not required	Ohio
Yes, for mail-in absentee voting: Okla. Stat. Ann. tit. 26, § 14-108	Yes for mail-in absentee voting: Okla. Stat. Ann. tit. 26, § 14-120; no for electronic transmission: § 14-118.1	After July 1, 2011, yes, photo not required	Oklahoma
Yes, for mail-in absentee voting: Or. Rev. Stat. § 253.070	Yes for mail-in absentee voting: Or. Rev. Stat. § 253.515; no for electronic transmission: § 253.690	No	Oregon
Yes, for mail-in absentee voting: 25 Pa. Stat. Ann. § 3146.6	Yes for mail-in absentee voting: 25 Pa. Stat. Ann. § 3146.6; electronic transmission not permitted	No	Pennsylvania
Yes, for mail-in absentee voting: R.I. Gen. Laws § 17-20-26	Yes for mail-in absentee voting: R.I. Gen. Laws § 17-20-22; no mention of security for faxed ballots: § 17-20-6.1	No	Rhode Island
Yes, for mail-in absentee voting: S.C. Code § 7-15-385	Yes for mail-in absentee voting: S.C. Code § 7-15-385; electronic transmission secrecy not discussed: § 7-15-460	Yes, photo not required. Photo ID law after preclearance from DOJ	South Carolina
Yes, for mail-in absentee voting: S.D. Codified Laws § 12-19-7	Yes for mail-in absentee voting: S.D. Codified Laws § 12-19-10; no electronic transmission permitted	ID requested, without ID affidavit required to cast regular ballot	South Dakota
Yes, for mail-in absentee voting: Tenn. Code Ann. § 2-6-202	Yes for mail-in absentee voting: Tenn. Code Ann.§ 2-6-502(f); no specific details of secrecy for electronic transmission of votes: § 2-6-502(e)	Yes, photo not required. Photo ID required after Jan. 1, 2012	Tennessee

State	Permit UOCAVA voters to return ballots electronically? (includes fax, e-mail, and Internet portal)	Permit *all* voters to return voted ballots electronically? (includes fax, e-mail, and Internet portal)	Require ballot secrecy for in-person voting?
Texas[c]	Yes, fax for military only in combat zones	No, mail or in-person only	Yes: Tex. Const. art. 6, § 4; disability exception: Tex. Elec. Code Ann. § 64.301
Utah[a]	Yes, e-mail and fax in combat zones	No, mail or in-person only	Yes: Utah Const. art. 4, § 8; disability exception: Utah Code Ann. § 20A-3-108
Vermont	No	No, mail or in-person only	Yes: Vt. Stat. Ann. tit. 17, § 2504; disability exception:
Virginia	No	No, mail or in-person only	Yes: Va. Const. art. 2, § 3; disability exception: Va. Code Ann. § 24.2-649
Washington[a]	Yes, fax only followed by submission of paper ballot	No, mail or in-person only	Yes: Wash. Const. art. 6, § 6; disability exception: Rev. Code Wash. § 29A.40.160
West Virginia	Yes, e-mail, fax, and Internet Pilot Program	No, mail or in-person only	Yes: W. Va. Const. art. 4, § 2; disability exception: W. Va. Code § 3-4A-22
Wisconsin[a]	No	No, mail or in-person only	Yes: Wis. Const. art. 3, § 3; disability exception: Wis. Stat. Ann. § 6.82
Wyoming	No	No, mail or in-person only	Yes: Wyo. Const. art. 6, § 11; disability exception: Wyo. Stat. Ann. § 22-13-113

Notes: Research is current to October 2011.

a = ID required for in-person voting but allows unsecure electronic voting

b = Photo ID required for in-person voting but allows unsecure electronic voting

c = ID required, photo required after DOJ preclearance for in-person voting but allows unsecure electronic voting

Require ballot secrecy for standard, absentee, or mail-in voting?	Require ballot secrecy for UOCAVA voting?	Require polling place voter ID? Photo required?	State
Yes, for mail-in absentee voting: Tex. Elec. Code Ann. § 86.005	Yes for mail-in absentee voting: Tex. Elec. Code Ann. § 86.005; yes for secret transmission of voted ballot electronically: § 105.001	Yes, photo not required. Photo ID law after preclearance from DOJ	Texas
Yes, for mail-in absentee voting: Utah Code Ann. § 20A-3-307	Yes for mail-in absentee voting: Utah Code Ann. § 20A-3-408; no for electronic transmission of voted ballots: § 20A-3-408.5(5)(a)	Yes, photo not required	Utah
Yes, for mail-in absentee voting: Vt. Stat. Ann. tit. 17, § 2543	Yes for mail-in absentee voting: Vt. Stat. Ann. tit. 17, § 2543; electronic transmission of voted ballots not permitted	No	Vermont
Yes, for mail-in absentee voting: Va. Code Ann. § 24.2-707	Yes for mail-in absentee voting: Va. Code Ann. § 24.2-707; electronic transmission of voted ballots not permitted	Yes, photo not required	Virginia
Yes, for mail-in absentee voting: Wash. Rev. Code Ann. § 29A.40.091	Yes for mail-in absentee voting: Wash. Rev. Code Ann. § 29A.40.091; yes for electronic transmission of voted ballots: § 29A.40.091(4)	Yes, photo not required	Washington
Yes, for mail-in absentee voting: W. Va. Code § 3-3-5	Yes for mail-in absentee voting: W. Va. Code § 3-3-5; no for electronic transmission of voted ballots: § 3-3-5(e)(2)(A)	No	West Virginia
Yes, for mail-in absentee voting: Wis. Stat. Ann. § 6.87	Yes for mail-in absentee voters: Wis. Stat. Ann. § 6.87; electronic transmission of voted ballots is not permitted	ID requested, not required to present until Feb. 2012 primary election	Wisconsin
Yes, for mail-in absentee voting: Wyo. Stat. Ann. § 22-9-113, 115	Yes for mail-in absentee voters: Wyo. Stat. Ann. § 22-9-113, 115; electronic transmission of voted ballots is not permitted	No	Wyoming

Notes

1. *See* Roy G. Saltman, The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence 160–69 (2006) [hereinafter Saltman]; *see also* Douglas W. Jones & Barbara Simons, Broken Ballots: Will Your Vote Count? 135–41 (2012) [hereinafter Broken Ballots] (reviewing examples of federal voting technology regulatory inadequacy and the certification of problematic voting systems).

2. The Help America Vote Act of 2002, 42 U.S.C. §§ 15301–15545 (2002) [hereinafter HAVA], provided financial incentives for state governments to replace mechanical voting equipment with electronic, computer-controlled systems. All statutory sections cited in the text or notes that omit full citation are HAVA sections. While HAVA did not explicitly mandate state transition to software-controlled systems, as a whole HAVA mandated particular functionality that was largely realized by electronic components. HAVA provided sufficient financial incentives and performance mandates so that e-voting was achieved virtually nationwide.

3. The U.S. Election Assistance Commission (EAC), http://www.eac.gov, generally follows the recommendations of the scientists at the National Institute for Standards and Technology (NIST) in approving qualified laboratories for conducting voting system testing. http://www.eac.gov/testing_and_certification/laboratory_accreditation.aspx. Collaboratively, the two agencies have substantially strengthened the qualifications for lab certification and for lab testing. *See id.* (linking to manuals that detail the requirements). These vital steps forward have unfortunately been undermined by a U.S. Department of Defense agency, the Federal Voting Assistance Program (FVAP), which had sought to sidestep the certification process in developing its voting system. See section titled *Litigation and Enforcement Strategies*.

4. Political scientists refer to the "residual vote rate" to describe the top-of-ballot electoral races that do not register a vote; this is often considered an indicator of voter balloting error. Stephen Ansolabehere and Charles Stewart III concluded, "If all jurisdictions in the United States that used punch cards in 2000 had used optically scanned ballots instead, we estimate that approximately 500,000 more votes would have been attributed to presidential candidates nationwide." *Residual Votes Attributable to Technology*, 67 J. Pol. 365–89 (2009). David Kimball analyzed the residual-votes data from the Ohio 2004 general election, disaggregating it by racial group and by income. Kimball concluded that

> systems without an error-prevention feature (e.g., punch card ballots and central-count optical scan ballots) produce a more dramatic increase in residual votes in counties with low median incomes and large percentages of African-American residents. By comparison, systems with an error-prevention feature (DRE voting machines and precinct-count optical scan ballots) do not yield such a dramatic increase in residual votes in counties with low median incomes or large African-American populations.

David C. Kimball, Expert's Report (submitted in support of plaintiffs in *ACLU of Ohio v. Brunner* 1, 11–12 (2008), http://moritzlaw.osu.edu/electionlaw/litigation/documents/ACLUOH-Motionforpreliminaryinjunction1-28-08AppD.pdf).

5. With few exceptions, HAVA requires voting systems used in federal elections to have the capacity to notify the voter of balloting errors, including overvotes (selecting too many choices for the race), and to permit the voter to correct the ballot before it is cast and counted. 42 U.S.C. § 15302.

6. The EAC maintains records of the locations using federally certified voting systems. At this writing, only a dozen of the over 7,000 local electoral jurisdictions have such voting systems deployed for 2012. *See* http://www.eac.gov/testing_and_certification/testing_and_certification_program.aspx (providing a map identifying locations of federally certified voting equipment). While HAVA required the creation of federal minimum standards and also a certification program, per HAVA § 15231(a)(2), state governments retain the power to ignore the federal "voluntary" standards and certification testing. But the states are nevertheless bound by the HAVA statutory minimums that are compulsory, not voluntary. *See* HAVA § 15481(a) (delineating mandatory requirements for all voting systems used in federal elections), http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx. Unfortunately, little legal attention has been dedicated to enforcing these mandatory provisions. *See infra Litigation and Enforcement Strategies.*

7. Fortunately, most absentee ballots will at least provide a voter-created record that can be recounted or audited. The vast number of absentee ballots not cast at polling locations or the election offices are marked on paper and returned via postal mail for conventional tabulation by optical scanning equipment. Some states, such as Ohio, define all early voting as "absentee," regardless of whether voters cast ballots in person at the local Board of Election during early voting periods. *See* Ohio Rev. Code Ann. §§ 3509.02, 3509.03 (West 2010).

8. *See* http://www.eac.gov/testing_and_certification/certified_voting_systems.aspx (last visited Feb. 20, 2012).

9. The most comprehensive and definitive of these scientific studies, the California Top to Bottom Review (TTBR) and the Ohio EVEREST assessment, reviewed multiple voting systems. Each of the reports submitted in these studies includes an Executive Summary written for lay readers lacking technical training. *See, e.g.*, the Source Code and Red Team Reports for Diebold/Premier, Sequoia, and Hart InterCivic voting systems, found at the California Secretary of State's website, http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm. One of the Ohio EVEREST reports, from the academic team, can be found at EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing (2007), http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf. The Ohio Secretary of State's office has removed several of the EVEREST reports, but the former Secretary Brunner's Executive Summary of all EVEREST reports (commercial vendors' and the academic experts', which basically confirm one another and the TTBR) is still available at http://www.sos.state.oh.us/sos/upload/everest/00-SecretarysEVERESTExecutiveReport.pdf (hereinafter Project EVEREST Executive Report). Some fair elections organizations have announced plans to post copies of all studies on their websites as a public library resource. For example, Verified Voting plans this step in an expanded online library. Conversation with the Verified Voting President, Pam Smith (July 2011). A shorter presentation of the EVEREST study focusing only on deficiencies of ES&S voting systems (the

nation's largest company and controlling more votes than any other system) can be found at Adam Aviv et al., *Security Evaluation of ES&S Voting Machines and Election Management System* (2008), http://micah.cis.upenn.edu/papers/aviv-evt08.pdf. A relatively comprehensive listing of the scientific studies conducted through 2008 with links to their public reports can be found 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 (2008), *available at* http://nob.cs.ucdavis.edu/bishop/notes/2008-forensic/index.html (providing a guide to indicators of possible electronic malfunctions and forensic assessments to determine whether the vote tabulation reports deserve trust).

The "tiny fraction" the text mentions has not yet been the subject of independent assessments. In the previous edition of *America Votes!*, the types of voting equipment problems that jurisdictions experienced in the 2008 presidential cycle and the scientific studies that had predicted the equipment's performance failures were inventoried. These deficiencies related to functional reliability, security from tampering, tabulation accuracy, and voter privacy. *See* Candice Hoke & David Jefferson, *Voting and Registration Technology Issues: Lessons from 2008*, *in* America Votes! 37–64 (Benjamin E. Griffith ed., Supp. 2009) [hereinafter *Voting and Registration Technology Issues*].

10. *See* Candice Hoke, *Judicial Protection of Popular Sovereignty: Redressing Voting Technology*, Case W. L. Rev. (Symposium; forthcoming summer 2012) (translating the definitive scientific and engineering assessments of voting system quality and security into legal concepts relevant to election law; noting that the premier scientists in the relevant field "have counseled the public and election officials that without other corrections and quality assurance steps, these machines are *unfit for voting*") (emphasis in original). Two definitive studies convened by state Secretaries of State explicitly translated the scientific findings. The California TTBR research team explained that their studies "demonstrated that the security mechanisms provided for all systems analyzed were *inadequate to ensure accuracy and integrity of the election results* and of the systems that provide those results." *Id.* (emphasis added). The EVEREST academic researchers' ultimate conclusion stressed, "All of the studied systems possess critical security *failures that render [them] insufficient to guarantee a trustworthy election*." *Id.* (quoting Project EVEREST Executive Report, *supra* note 9, at 35). It is not that the vote totals will always be accurate or inaccurate. The voting system software does not report when it has erred or been modified surreptitiously and when it is accurate. Unless producing an "implausible" error (*see* Ellen Theisen, *Ballot-Scanner Voting System Failures in the News—Partial List*, VotersUnite.Org (May 22, 2009), *available at* http://www.votersunite.org/Info/OpScansInTheNews.pdf), such as more total ballots cast than registered voters, no indicators may surface. Thus, software bugs, tampering, or even election officials' and voters' inadvertent errors with the equipment can produce erroneous tallies that can lead to structural disenfranchisement of the voting public or some subset. Currently, other than a few statistically sound post-election auditing programs, election officials are not required to check on the accuracy of the machine-generated results. In other states (e.g., Virginia), laws prohibit manual recounts, the only effective current check on the machine counts. Florida conducts "recounts" by using the same software-produced precinct results, which cannot identify a software problem with the count.

11. *Voting and Registration Technology Issues, supra* note 9, at 37–58 (reviewing the record of voting system dysfunctions during the 2008 primary and general election cycle). Few jurisdictions have changed voting system equipment since 2008.

12. The vendors have compensated computer scientists to serve as experts. They have claimed that use of the software is "reasonable," implying that a low rate of errors occurs. *See, e.g.*, defendants' expert reports submitted in Schade v. Md. State Bd. of Elections, 930 A.2d 304, 328 (Md. 2007) (deferring to the state board of elections' judgment in certifying DREs that lacked a voter verified paper audit trail), and in Gusciora v. Corzine, No. MER-L-2691-04, 2010 N.J. Super. LEXIS 2319 (N.J. Super. Ct. Law Div. 2010) (holding that state's certification of direct recording electronic (DRE) voting units did not violate voters' state constitutional rights). But the supposed scientific experts have not revealed that no comprehensive statistical study of the error rates of this voting equipment in actual elections has occurred, nor even of the error rates in some elections where errors in the final tabulations have been documented. No authoritative power—courts, the EAC, or state Secretaries of State—have convened a study independent of the vendors to determine error rates produced by the equipment in the field as used in real elections.

The *Schade* court additionally credited the supposed "accessibility" of the electronic equipment, but that ruling was not based on qualified testimony but apparently on the marketing representations by vendors. By contrast, when a qualified accessibility engineer with over three decades of experience in developing and testing assistive technologies tested the "accessible" voting devices with volunteer voters of varying physical needs, he documented their failures to satisfy the legal requirements for accessibility as well as their abject failure in meeting security standards. *See infra* note 163 (reviewing accessibility engineer Noel Runyan's studies).

13. 42 U.S.C. §§ 15301–15545.

14. *See supra* note 5.

15. The National Association of Secretaries of State (NASS) has repeatedly called for the EAC's termination, most recently in 2011, when it voted to establish a task force on reallocating the EAC's legal duties to other agencies. *See NASS Resolution Establishing a Task Force on the Future Disposition of EAC Duties* (July 13, 2011), http://www.nass.org/index.php?option=com_content&view=article&id=87&Itemid=386. The controversy over the EAC's contracted voter fraud study provided one flash point. *See* Rick Hasen, *Indiana Secretary of State Rokita, the EAC Controversy, and the Incidence of Voter Fraud*, Election Law Blog (Apr. 11, 2001), http://electionlawblog.org/archives/008228.html. The EAC Inspector General reports have detailed an assortment of legal infractions and nonfeasance. *E.g., Report of Investigation: Preparation of the Voter Fraud and Voter Intimidation Report*, U.S. Election Assistance Commission, Office of Inspector General (March 2008), *available at* http://www.eac.gov/assets/1/Page/EAC%20Inspector%20General%20Report%20on%20the%20Preparation%20of%20the%20Voter%20Fraud%20and%20Voter%20Intimidation.pdf. *See generally Office of Inspector General Reports*, U.S. Election Assistance Commission, http://archives.eac.gov/eac_ig/reports-folder (last visited Mar. 18, 2012). This author considers the EAC in need of structural reform and reconstitution to be a technically capable entity, with appropriate computer security and usability engineering knowledge at every level, on a bipartisan basis.

16. The EAC has advised on the scope of its activities while it lacks Commissioners. http://www.eac.gov/blogs/work_continues_at_the_eac/. In January 2012, the EAC's combination Acting Executive Director and General Counsel issued a memo directing the EAC's 37-member Board of Advisors and 110-member Standards Board to cease all official activities, at http://www.eac.gov/about_the_eac/eac_advisory_boards.aspx.

17. As this chapter goes into print, President Obama's proposed budget includes an appropriation for the EAC. http://blog.lib.umn.edu/cspg/peea/images/EAC.FY13.Pres.budget.request.pdf (last visited Feb. 13, 2012). Despite NASS's resolutions calling for termination of the EAC, even more recently NASS passed a resolution calling for the continued activities of the EAC Standards Board and Board of Advisors. NASS referred to these Boards as "essential to the continued development of standards for election administration." *NASS Resolution on the Continued Functioning of the EAC Standards Board and Board of Advisors* (Jan. 28, 2012), http://www.nass.org/index.php?option=com_content&view=article&id=87&Itemid=386. Professor Rick Hasen blogged about the "hypocrisy" shown by these two resolutions, but they can be reconciled. The July 2011 resolution calling for EAC termination was passed on the last day of the NASS conference after more than a majority of the Secretaries had departed, and was not listed as an action item on the NASS agenda. The January 2012 resolution reflects the judgment of a majority of Secretaries, and evidently a commitment to EAC's continuation in some form.

18. *Voting and Registration Technology Issues*, *supra* note 9.

19. A systematic critique of the federal regulatory structure addressing voting technologies is beyond the scope of this chapter. *Voting and Registration Technology Issues*, *supra* note 9, *passim* addresses some of these deficiencies.

20. While HAVA is silent on private rights of action to enforce these standards, litigation will undoubtedly ensue to affirm these powers to enforce civil rights within the electorate instead of only partisan-connected leaders. 42 U.S.C. § 15511 (detailing the Attorney General's powers to enforce the minimum "uniform and nondiscriminatory election technology and administration requirements" detailed in specified HAVA sections that include § 15481, Voting Systems Standards).

21. *See* P.B. Stark & D.A. Wagner, *Evidence-Based Elections*, IEEE Security and Privacy, http://statistics.berkeley.edu/~stark/Preprints/evidenceVote12.pdf (pre-publication version; publication forthcoming 2012) [hereinafter *Evidence-Based Elections*]. Their paper proceeds from the premise that under current software development processes and as documented in definitive voting system studies, software-based voting systems cannot provide high assurance that election results are accurate. But the results *may* be accurate and can be verified using statistically valid, relatively rapid methods.

Scientists Ron Rivest and John Wack first developed the concept and justification for a "software-independent" verification of election results as part of the EAC's development of voting systems standards. *See* R. Rivest, *On the Notion of "Software Independence" in Voting Systems*, 366 PHIL. TRANSACTIONS ROYAL SOC'Y A, 3759 (2008) (explaining its use as remedy for errors endemic to computer-based elections systems).

Professors Phillip Stark and David Wagner elaborate Rivest's and Wack's foundational concept:

> A voting system is *strongly software-independent* if an undetected error or change to its software cannot produce an undetectable change in the outcome, and we can find the correct outcome without re-running the election. Strong software-independence does not mean the voting system has no software; rather, it means that even if its software has a flaw that causes it to give the wrong outcome, the overall system still produces "breadcrumbs" (an audit trail) from which we can find the true outcome, despite any flaw in the software. Systems that produce voter-verifiable paper records (for instance, voter marked paper ballots) as an audit trail are strongly software-independent, provided the integrity of that audit trail is maintained, because the audit trail can be used to determine the true outcome.

Evidence-Based Elections at 2 (emphasis added).

22. A DRE is a direct recording electronic voting unit that digitally records voters' choices. The current generation of DREs tends to feature a touchscreen as the mechanism on which voters indicate their choices, theoretically translated into electronic signals that enter votes into the electronic "buckets" for each candidate consistent with the voters' choices. Independent testing has shown that these all-electronic units can be made to "cheat"—either deliberately by human tampering or inadvertently because of buggy software or other defects. *See* the California TTBR of voting systems, http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm, and the Ohio EVEREST assessments, http://siis.cse.psu.edu/everest.html (last visited Feb. 11, 2012). The iVotronics DREs' alleged flaws generated the hotly contested Florida-13 congressional race that resulted in numerous investigations and litigation. Jennings v. Elections Canvassing Comm'n of Fla., 958 So. 2d 1083 (Fla. Dist. Ct. App. 2007); Government Accountability Office (GAO), *Further Testing Could Provide Increased but Not Absolute Assurance That Voting Systems Did Not Cause Undervotes in Florida's 13th Congressional District*, GAO-08-97T (Oct. 2, 2007), http://www.gao.gov/assets/90/82321.pdf.

23. South Carolina uses all-electronic DRE touchscreen voting devices, specifically the ES&S iVotronic, that do not produce an independent paper record to provide a check on the computer's software-recorded votes and tabulations. *See* Duncan Buell, E. Hare, F. Heindel, C. Moore & B. Zia, *Auditing a DRE-Based Election in South Carolina*, Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE'11) (Aug. 2011) [hereinafter S.C. *League*].

24. The Bradblog reported, "Lancaster County *paper* absentee ballots went to Rawl 84% to 16%. The unverifiable touch-screens in the same county, however, said Rawl lost the county by 17%. Greene received *more votes than were cast in 25 Spartanburg County precincts*. The *votes of 50 other precincts were missing from the final count*. Statewide, the virtually unknown Greene somehow managed to captured 60% of the vote, according to the iVotronic DREs." http://www.bradblog.com/?p=8796 (initial emphasis in original, the remainder emphases added). David Axelrod, President Obama's senior advisor, commented, "The whole thing is odd. . . . I don't really know how to explain it, and I don't think anybody else does either." Brian Knowlton, *More Questions About Mysterious South Carolina Senate Candidate*, http://thecaucus.blogs.nytimes.com/2010/06/13/more-questions-about-mysterious-south-carolina-senate-candidate/.

25. A widely remarked disparity lay in the proportion of paper ballot absentee ballot votes for each candidate versus the electronic ballots cast on Election Day at the polls with no auditable record. "House Democratic whip James Clyburn of South Carolina has called for a federal investigation into the 'shenanigans' and claims up to three state races may have been tampered with." Patrik Jonsson, *South Carolina Head Scratcher: More Curiosities in Election of Alvin Greene* (June 12, 2010), http://www.csmonitor.com/USA/Politics/2010/0612/South-Carolina-head-scratcher-More-curiosities-in-election-of-Alvin-Greene. The *Christian Science Monitor* reported that the strongest Democratic candidate seeking to be GOP Senator DeMint's general election opponent, Vic Rawl, had been rated highly competitive because he was trailing in opinion polling by only single digits. "Republicans feared DeMint's seat was not, in fact, secure and a progressive insurgency could put Rawl ahead of him in November." *Id.* A mathematician compared the statewide Democratic primary races and found the electronic and paper absentee ballot ratios anomalous only in this race. K. Dopp, *South Carolina 2010 Democratic United States Senate Primary Election*, http://kathydopp.com/wordpress/?p=98 (last visited Feb. 10, 2012). Rawl's post-election statistical experts noted anomalies; Rawl did "significantly better in absentee paper ballots than on Election Day. 'In 10 counties we did 20 percent better. In one county we did 43 percent better. We looked at the other races on the ballot and that wasn't the case. . . . In 25 precincts in one county, *Greene got more votes than were reported to have been cast*,'" referring to Spartanburg County. "In 50 other precincts in that county, votes were missing." *Election Expert, Opposition Campaign Suspect Foul Play in S.C. Primary*, Newsweek Daily Beast, June 11, 2010 (emphasis added). *But see* Joseph Bafumi, Michael C. Herron, Seth J. Hill & Jeffrey B. Lewis, *Alvin Greene? Who? How Did He Win the United States Senate Nomination in South Carolina?*, http://www.dartmouth.edu/~herron/greene.pdf (working paper 2010) (arguing that statistical analysis shows the apparent anomalies to be within the range of normal disparities between absentee and in-person voting).

26. Although one deficiency of the all-electronic DRE voting devices defeats effective audits of whether the machine accurately recorded each voter's selections, the League of Women Voters was able to audit a different task: whether the countywide reported tabulations of results reflected vote records from every voting device used in the election. The tabulations were often incomplete. *See S.C. League, supra* note 23.

27. Peggy J. Brown & Barbara Zia, *Can the State Election Commission Do Its Job?*, The State (Columbia, S.C.), http://www.thestate.com/2011/08/24/1944276/brown-zia-can-state-election-commission.html [hereinafter Brown & Zia]. *See also S.C. League, supra* note 23.

28. Brown & Zia, *supra* note 27. Note that counting some voters' ballots more than once ineluctably dilutes the voting weight of other voters' cast ballots and thus generates vote dilution proscribed by law. *See* Allen v. State Bd. of Elections, 393 U.S. 544, 569 (1969) (citing Reynolds v. Sims, 377 U.S. 533, 555 (1964), and noting, "The right to vote can be affected by a dilution of voting power as well as by an absolute prohibition on casting a ballot.").

29. *See, e.g.*, *County Blames ES&S Software for Error in Vote Totals*, http://eyeonwilliamson.org/?p=648 (providing materials from *System Counts Too Many Votes*, Taylor Daily Press, Nov. 16, 2006, regarding Williamson County, Texas, vote totals that were roughly three

times greater than the number of voters casting ballots and reporting that ES&S claimed human error in the county).

30. The U.S. Department of Justice (DOJ), Antitrust Division, joined by nine states, sued vendor Election Systems and Software, Inc., for violations of Section 7 of the Clayton Act, 15 U.S.C. § 18, caused by the corporation's covert purchase of the former Diebold/Premier election systems division. By this purchase, ES&S sought to merge the nation's largest and second-largest voting system companies, whose combined market share would allow their software to control the ballots cast by over 73 percent of all U.S. voters. A comprehensive consent decree issued compelled divestiture. *See* United States v. Election Sys. & Software, Inc., 722 F. Supp. 2d 117 (D.D.C. 2010) (Final Judgment); http://www.justice.gov/atr/cases/f256200/256275.htm (complaint). The DOJ claimed success in the action, http://www.justice.gov/atr/public/press_releases/2010/256267.htm.

The DOJ has not been involved, however, in enforcing HAVA's requirements for voting system accuracy and auditability, even if proof of inaccuracy has been generated. *See infra Litigation and Enforcement Strategies*. For instance, ES&S attempted to block a forensic audit of the Venango County, Pennsylvania, local election in 2011 that the county Board of Election claimed was pervaded with anomalies. The vendor claimed that its proprietary trade-secret software would not be sufficiently protected in an audit. Media reported that the company had sent threatening legal letters to both the county and the two computer scientists acting as auditors. ES&S warned that the county would face a lawsuit unless it agreed to complete confidentiality and that results of the analysis would not be publicly released without the company's prior review and approval. A preliminary audit report issued, however, establishing that among the electronic records proof existed that someone had used a computer that was not a part of the county's election network to remotely access the central election tabulator computer, illegally, "on multiple occasions." http://www.bradblog.com/?p=8874.

31. HAVA requires auditability of all voting systems used in federal elections. *See* HAVA § 301. The funding for procuring the vast majority of these ES&S voting machines was HAVA monies, yet the company has engaged in only *de minimis*, perfunctory efforts to render them auditable. When forensic audits of the equipment as used in live elections have been sought, the company routinely opposes the efforts on trade-secret grounds, which are arguably excluded by HAVA's insistence on auditability and by other election law protecting the right to vote.

32. Unfortunately, even though extrinsic evidence demonstrated substantial errors and omissions, the Commission declined to modify the totals. For instance, Colleton County's tabulation equipment errors were identified but not corrected in the certified count. "The certified returns, accepted by the county and the State Election Commission, contained several contests in which the *sum of the votes for the candidates exceeded the number of votes cast in the county, some by more than 10%*. A third tabulation released by the Election Director in Colleton County at the end of December, 2010, repaired some problems but *in several races the number of absentee votes still exceeded the number of absentee ballots*." South Carolina Voting Information, Final Numbers for Colleton County, http://www.scvotinginfo.com/wp/2011/04/18/final-numbers-for-colleton-county/#more-747 (emphasis added).

33. *See supra* note 22 (defining DRE voting device).

34. Probably the most notorious controversy concerned the Florida congressional district 13 in 2006. Jennings v. Elections Canvassing Comm'n of Fla., 958 So. 2d 1083 (Fla. Dist. Ct. App. 2007). The more recent effort by ES&S, iVotronic's manufacturer, to block a forensic audit of the flawed elections conducted in Venango County, Pennsylvania, has received significant publicity. *See, e.g.*, http://www.scvotinginfo.com/wp/2011/10/04/venango-county-pennsylvania-decides-to-vote-with-paper-not-ivotronics/, http://www.truth-out.org/election-systems-software-attempts-block-independent-audit-failed-touch-screens/1320081165; *Forensic Analysis Finds Venango County E-Voting System "Remotely Accessed" on "Multiple Occasions" by Unknown Computer*, http://thevotingnews.com/blogs/forensic-analysis-finds-venango-county-pennsylvania-e-voting-system-remotely-accessed-on-multiple-occasions-by-unknown-computer-the-brad-blog/.

35. The popularly used term embracing both optical scan ballots and DRE-paper records of cast ballots has become "voter-verified paper record." *See, e.g.*, Statement of Rep. Rush Holt to the New Jersey Senate, http://www.verifiedvotingfoundation.org/article.php?id=6667; Verified Voting's report of Robert Kibrick, *Voter-Verified Paper Record Legislation*, http://www.verifiedvoting.org/article.php?list=type&type=43. Verified Voting maintains an inventory of voting technologies used in the United States, classified by state, at http://www.verifiedvoting.org/verifier/; it identifies states using verifiable paper ballot records.

36. *See Voting and Registration Technology Issues, supra* note 9; Voters' Unite and Common Cause, *A Master List of 70+ Voting Machine Failures and Miscounts by State*, http://www.commoncause.org/atf/cf/%7Bfb3c17e2-cdd1-4df6-92be-bd4429893665%7D/MASTERLISTOFMACHINEFAILURES.pdf [hereinafter *Master List*].

37. South Carolina, which uses only one vendor statewide (ES&S), has experienced a multitude of other embarrassing, mission-critical voting system failures. *See supra* notes 22–36 and accompanying text; *see also Voting and Registration Technology Issues*, supra note 9, at 41.

38. No reported opinion exists, but Andrew Appel's blog postings provide an overview of the issues and the judicial order issued in *In re Petition of Zirkle, sub nom. Zirkle v. Henry*, No. Cum-L-000567-11-A, N.J. Super. Ct. Law Div., hearing and bench order Sept. 1, 2011, *transcript available at* http://www.cs.princeton.edu/~appel/voting/zirkle-transcript-1sep11.pdf. *See* Andrew Appel, *New Jersey Election Coverup*, https://freedom-to-tinker.com/blog/appel/nj-election-cover; Appel's expert report in the case, http://www.cs.princeton.edu/~appel/voting/zirkle-appel-certif2.pdf [hereinafter Zirkle Report]. *See also* Appel blog, *Corruption Bureau Assigns Fox to Guard Henhouse*, discussed *infra* notes 40–42 and accompanying text.

39. *See* Zirkle Report, *supra* note 38, at 2–8.

40. New Jersey's all-electronic DRE voting machines have faced constitutional challenges and prior forensic exams. The importance of Professor Appel's expert report filed in the ongoing state constitutional challenge to the DRE voting systems, *Gusciora v. McGreevey*, http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/voting/advantage/appel-expert-report-unredacted.pdf, continues. Professor Appel chairs the Princeton Computer Science department and is a widely recognized national expert in computer security, unlike the experts that the state impaneled and the Court qualified. Appel has conducted forensic studies of New Jersey's most common DRE systems, documenting a range of serious flaws that undermine their capacity to produce accurate election tallies. Rutgers Law

Professor Penny Venetis, who represents the plaintiffs in *Zirkle* (discussed in the text) and in *Gusciora v. McGreevey*, 2010 WL 444173 (N.J. Super. Ct. Law Div. 2010), has filed an appeal challenging the trial court's judgment that the DRE vulnerabilities could be managed effectively to prevent tampering and to protect accurate elections, and that thus the DREs did not require replacement (copy of appeal documents on file with author).

41. Several of the state of New Jersey's witnesses claimed that tampering was virtually impossible. The court recounts these disputations of significant vulnerabilities in *Gusciora v. McGreevey*, 2010 WL 444173. The Court's opinion demonstrates that the judge relied on the highly compensated computer experts who held law degrees more than on those who held the requisite knowledge in computer security. While she ordered the state to undertake a wide range of mitigations designed to reduce their vulnerability to tampering, when the state did not perform, the Court continued to offer continuances rather than sanctions or compliance. An appeal is pending.

42. At the time this book went to press, *Zirkle* had not been fully resolved. Appel's blog entry entitled *Corruption Bureau Assigns Fox to Guard Henhouse*, recounts the events in the ongoing New Jersey dispute. https://freedom-to-tinker.com/blog/appel/corruption-bureau-assigns-fox-guard-henhouse (Sept. 28, 2011).

43. The official continued, "[This] may not be a problem in counties where a very large volume of ballots are counted, but in our county, where we typically process 2,500 or less, the margin of error can greatly affect the outcome of the race." Discussing other irregularities, the Board noted, "After the second stack of ballots for precincts was run through the machine . . . , the voting device failed to accept the disk, generating this message: 'Counters have reached maximum. Counters restored to last batch saved.' Therefore, the backups required by the security conditions from the SOS for the M650 were not done." Teresa Benns, *Canvass Board Answers Complaint* (Apr. 3, 2011), http://www.examiner.com/conservative-in-colorado-springs/canvass-board-answers-complaint. Notably, the M-650 central-count, high-speed scanner (manufactured by ES&S) is one of the most broadly deployed central-count scanners nationwide.

44. *Id.*

45. The central-count, high-speed optical scanner M-650 is manufactured and marketed by ES&S, the nation's largest voting system vendor.

46. *See* Final Report of the Cuyahoga Election Review Panel 5–7 (2006), http://urban.csuohio.edu/cei/public_monitor/CERP_Final_Report_20060720.pdf.

47. *Id.* at 13–67 (reviewing vendor marketing, the executed contracts, and the unfulfilled vendor promises).

48. Gregory Korte, *Federal Agency Finds Defects in Ballot Scanners*, USA TODAY, Dec. 22, 2011, http://www.usatoday.com/news/politics/story/2011-12-22/defective-voting-machines/52172034/1?loc=interstitialskip (last visited Jan. 30, 2012) (noting three problems: (1) random screen-freezes that prevent ballots from being fed; (2) failure to log errors in a file that would let election officials know of problems; and (3) skewing of ballots as fed into the machine, making votes unreadable if marked in some ballot areas). Unfortunately, these vendor problems imposed additional costs on the taxpayer: "the Cuyahoga County elections director said the county had to switch to shorter ballot pages to fix the problems, and later reached a $208,197

settlement with the company. Later fixes offered by ES&S also led to system freezes, so the county went back to the previous, flawed software as 'the devil we know,' she said."

49. *EAC Issues Formal Investigation Report on DS200 Precinct Count Optical Scanner* (Dec. 22, 2011), http://www.eac.gov/blogs/eac_issues_formal_investigation_report_on_ds200_precinct_count_optical_scanner/.

50. Bill Hess, *Computer Glitch Causes Hiccup in Cochise County Tally,* Wick News Service, http://www.douglasdispatch.com/articles/2008/02/07/news/doc47ab6bc4d0b70550988123.txt (last visited Mar. 8, 2012). Cochise County used ES&S voting systems with its Unity software for ballot design and tabulation.

51. The Director of Butler County elections commented, "Quite frankly, if it's off by five votes or 105 votes, I want to know what's causing it. Especially if it's a close election," McGary said. "If we cannot produce accurate and reliable numbers, then it throws the entire process in question, and that's not something we want to have happen." Jon Craig, *Butler County Missed 105 Votes,* Cincinnati Enquirer, *archived at* http://www.votersunite.org/article.asp?id=7628. The County's letter to the vendor stated, "A situation of this nature could impact any election. It may appear that every vote has been counted when cards indicate they are being properly uploaded, when in fact votes cast on a memory card(s) are not tabulated in the results." *See* Bradblog, *Failed Again: Widely-Used Diebold Touch-Screens Systems Dropped Votes in Recent Ohio Primary,* http://www.bradblog.com/?p=5879 (appending copy of County letter).

52. While the EAC has the statutory duty of conducting an Election Day Survey, and in 2004 included a few questions regarding voting system performance, inexplicably the questions were deleted from surveys prepared for 2006 and 2008 federal elections. Susannah Goodman testified before the EAC on this point, noting:

> Election Data Services, the contractor who compiled the [2004] survey results, recommended the EAC expand collection of data on voting system performance, stating, "We recommend that the EAC institute a more extensive program designed to investigate reported voting equipment problems . . . with wide ranging rumors and reports of voting equipment problems that came out of the 2004 election, there is a lack of full information to substantiate or dispel the rumors." Unfortunately, questions on voting machine performance have been removed from both or were just not put into the 2006 and 2008 surveys.

Remarks of Susannah Goodman, Director of Common Cause Democracy Program, Transcript of the EAC Meeting, at 77 (Dec. 8, 2008), http://www.eac.gov/assets/1/AssetManager/transcript%20public%20meeting%20december%208%2020081.pdf [hereinafter Goodman Testimony].

Three voting system inventories of malfunctions or "incidents" have been generated by nonprofit research and advocacy organizations. These provide organized listings by state of incidents that undermined the voting system's functional performance in elections, including its accuracy: (1) a malfunction and miscount list by Common Cause and Voters Unite!, *Master List, supra* note 36; (2) the Voters Unite study of errors attributable to ballot-scanning technology, *see* Ellen Theisen, *Ballot-Scanner Voting System Failures in the News—A Partial List,* VotersUnite.Org (May 22, 2009), *available at* http://www.votersunite.org/Info/OpScansInTheNews.pdf; (3) the most recent inventory, Lawrence Norden, *Voting System Failures: A Database Solution*, Brennan Center for Justice at New York University School of Law 14 (2010) (collecting incidents of miscounts and malfunctions in Appendix 2), *available at* http://www.brennancenter.org/content/resource/voting_system_failures_a_database_solution/. The VotersUnite scanner study was designed to demonstrate that these devices are not panaceas but equally afflicted with buggy software and security failings that can produce a false confidence in their accuracy. Scanners do, however, offer a critical difference: they require a voter-marked paper ballot that can be retabulated by hand or by a validated scanner, and thus serve as a check on flawed software.

Many of these "incidents" of failure or miscounts, such as those noted in the text, relate to software design or coding flaws and thus affect voting systems nationwide even if the local election officials have not noticed any significant discrepancy in their own vote totals. But unless implausible or systematically audited, the machine totals will normally not produce any indicators of even grossly erroneous tabulations. Inadvertent or deliberate vote flipping between candidates and other errors will thus not be caught and corrected. There are no hard data showing the overall rates and trends of voting system malfunctions and tabulation errors, and despite its need, the EAC has not been collecting the data in its Election Day survey. *See* Goodman Testimony, *supra*, and following colloquy with Commissioners.

53. The EAC held a hearing on whether the agency needed to develop a comprehensive voting system incident reporting system. Florida Secretary of State Kurt Browning, New York State Board of Elections Co-Chair Douglas Kellner, Michigan Director of Elections Chris Thomas, and this author testified before the EAC on the question. *See Minutes of the Public Meeting*, U.S. Election Assistance 97–148 (Dec. 8, 2008), http://www.eac.gov/assets/1/AssetManager/transcript%20public%20meeting%20december%208%2020081.pdf. Three of the four witnesses urged the EAC to develop a reporting system on equipment currently deployed, regardless of whether the EAC had certified it as compliant with the EAC's own standards. *See* Candice Hoke, *Tracking Voting Technology Field Performance: The Federal Role*, Public Hearing of U.S. Election Assistance Commission, Washington, D.C. (written testimony in advance of Dec. 8, 2008 hearing) (outlining some crucial features and justifications), http://www.eac.gov/assets/1/AssetManager/testimony%20candice%20hoke%20center%20for%20election%20integrity%20public%20meeting%20december%208%202008.pdf. The Brennan Center for Justice published its comprehensive report outlining a feasible solution, *see* Norden, *Voting System Failures*, *supra* note 52 (outlining a feasible incident tracking system that provides broad public access and support to election officials and policy makers).

54. 531 U.S. 98 (2000).

55. *See* 42 U.S.C. § 15481(a)(5).

56. *See id.* § 15481(a)(2). The manual audit capacity requirement arguably requires a paper record that must be created contemporaneously with the voter's ballot casting. It can then be used as a check on the invisible electronic record via recounts and other auditing methods that provide software-independent verification of the computer-generated results.

57. The *per curiam Bush v. Gore* opinion, 531 U.S. at 111, noted, "Nationwide statistics reveal that an estimated 2% of ballots cast do not register a vote for President for whatever

reason . . . ." *See also* Caltech/MIT Voting Technology Project, *Residual Votes Attributable to Technology: An Assessment of the Reliability of Existing Voting Equipment* 11 (displaying *Table 3*, Residual Vote as a Percent of Total Ballots Cast by Machine Type and Year U.S. Counties, 1988–2000 Presidential Elections), http://vote.caltech.edu/drupal/files/report/residual_votes_attributable_to_tech.pdf (Mar. 30, 2001).

58. 531 U.S. at 105–10. The Court observed, "Equal protection applies as well to the manner of its exercise. Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another." *Id.* at 104. The Court held that the judicial order to proceed with the recount despite the omission of a consistent standard as to what marks would count as a valid vote violated this constitutional principle. *Id.* at 109–10.

Commentators have contended that a range of factors other than those the Court directly mentioned influenced the Court's decision. Paul Schwartz has offered one of the most persuasive assessments of the underlying epistemological approaches of the different voting blocs. He suggests that the Justices favoring the continuation of the recount perceived election technology as a fallible instrument for converting voters' choices into votes. By contrast, the Court's majority placed greater trust in the machines over fallible and conflicted or biased humans. The more conservative voting bloc sought hard-edged rules to constrain election officials' discretion and thereby avoid these human imperfections. *See* Paul M. Schwartz, *Voting Technology and Democracy*, 77 N.Y.U. L. Rev. 625 (2002).

59. Bush v. Gore, 531 U.S. 98.

60. *Id.* These questions included whether Florida had denied its citizens equal protection and substantive due process under the Fourteenth Amendment when Florida counties used varying legal standards for determining a valid punch-card vote.

61. The incapacity of the punch-card voting equipment to consistently count overvotes was one problem, but another lay in the problematic butterfly ballot designs that some counties used, arguably causing high overvoting rates. *See* Barry H. Weinberg & Lyn Utrecht, *Problems in America's Polling Places: How They Can Be Stopped*, 11 Temp. Pol. & Civ. Rts. L. Rev. 401, 429–30 (2002):

> Perhaps the most prominent allegation of flawed ballot design is the now infamous "butterfly ballot" in Palm Beach County Florida. The design of the ballot was such that many people were uncertain which hole to punch for the candidate of their choice. In other instances, voters believed that they might have punched the wrong hole.

See also Erwin Chemerinsky, *How We Should Think About* Bush v. Gore, 34 Loy. U. Chi. L.J. 1, 10 (2002) ("The ballot in Palm Beach County was constructed in a misleading manner: the hole next to Gore's name was actually a vote for Patrick Buchanan. This resulted in approximately 4000 Palm Beach County voters mistakenly casting their votes for Buchanan, though intended for Gore. This, of course, was far more than the margin of Bush's victory and more than enough to have made Gore the clear winner in Florida.").

62. HAVA, 42 U.S.C. § 15302.

63. Optical scanners record and tabulate paper ballots after voters ink their selections. Other ballots may be electronic, designed for voters to select their choices and record their votes on computer-based equipment that tabulates votes by software applications. *See generally* Doug Jones, *A Brief Illustrated History of Voting*, http://www.cs.uiowa.edu/~jones/voting/pictures/; SALTMAN, *supra* note 1.

64. Increased accessibility for voters with disabilities and reduction of uncounted votes (owing to "overvoting") are the chief achievements. *See* R. Michael Alvarez et al., *2008 Survey of the Performance of American Elections: Final Report*, MIT-Cal Tech Voting Project, www.vote.caltech.edu/drupal/files/report/Final%20report20090218.pdf.

65. The EAC has posted a map of locations with EAC-certified voting systems; in October 2011, only 10 local jurisdictions were listed. http://www.eac.gov/testing_and_certification/default.asp.

66. *Id.*; *see* BROKEN BALLOTS, *supra* note 1.

67. *See infra* text accompanying notes 94–100.

68. Technical reliability and security, tabulation accuracy, and voter privacy/ballot secrecy are some areas of continuing performance deficiencies. *See supra* note 9 (regarding the TTBR and EVEREST studies); *see also Voting and Registration Technology Issues*, *supra* note 9; BROKEN BALLOTS, *supra* note 1.

69. Florida has initiated many changes in its procedures and voting systems since the fateful 2000 election. *See* Kenneth Tinkler, *Florida Election Procedural and Legal Changes from 2000 to 2008: A Primer*, *in* AMERICA VOTES! 19–36 (Benjamin Griffith ed., Supp. 2009).

70. *See, e.g.*, LORRAINE C. MINNITE, THE MYTH OF VOTER FRAUD (2010), and works referenced therein.

71. The Lawyers' Committee for Civil Rights Under Law, the Advancement Project, and the Brennan Center for Justice maintain research projects and litigation efforts to redress voter ID and partisan-animated voter suppression.

72. Among those who sustain a focus on the election technology issues are election officials and their lawyers, fair elections nonprofit advocacy organizations, and voting system vendors. Others who lack technical security competence will often advocate new ways to use information technologies to advance their agendas without comprehending the security risks. *See, e.g.*, *Americans Elect Internet Vote for President? Consider How It Worked in DC 2010*, http://irregulartimes.com/index.php/archives/2011/07/25/americans-elect-Internet-vote-for-president-hacked-in-dc-2010/ (criticizing Americans Elect for seeking to conduct an Internet-based 2012 presidential nominating election without understanding or disclosing the inability to control the security risks that can lead to a falsified election).

73. An "Archimedean point" refers to a hypothetical standpoint from which totally objective and impartial assessments are possible, not subject to the flawed perceptions and biases normally characteristic of human judgment. *See* HANNAH ARENDT, THE HUMAN CONDITION 11, 262–68, 322–23 (1958) (cautioning against using this approach when human judgment is needed); *see also* MICHAEL J. SANDEL, LIBERALISM AND THE LIMITS OF JUSTICE 17 (1982); JOHN RAWLS, A THEORY OF JUSTICE 21–22 (1971) (advancing the need for a "standpoint . . . to envision our

objective from afar"); Pieter Tijmes, *The Archimedean Point and Eccentricity: Hannah Arendt's Philosophy of Science and Technology*, 35 INQUIRY 389 (1992).

74. 42 U.S.C. §§ 15301–15545 (2002). Curiously, in enacting HAVA, Congress supplied none of the common sources of legislative history. No committee reports accompanied the final versions of the bill.

75. Bush v. Gore, 531 U.S. 98, 111 (2000).

76. For instance, ballot secrecy is designed to protect voters from coercion and retribution for their votes, functioning as a systemic protection for free elections. Elections separate the identity of the voter from his or her cast ballot, whereas in virtually all other applications, including financial services and commercial sales, the customer can be tracked and individualized audits can occur.

77. HAVA does transfer the Federal Election Commission powers under the National Voter Registration Act to the EAC, which includes a slight amount of regulatory authority. *See* HAVA, 42 U.S.C. § 15532.

78. *See, e.g.*, 42 U.S.C. §§ 15381–15387, 15501. The EAC website observes, "One of EAC's top priorities is providing assistance to election officials. EAC has issued guidance, advisories and best practices to help officials comply with HAVA and make other election administration improvements and enhancements." *Election Management Resources*, U.S. ELECTION ASSISTANCE COMMISSION, http://www.eac.gov/election_management_resources/default.aspx (last visited Mar. 18, 2012).

79. U.S. CONST. art. I, § 4.

80. These positions are somewhat reflected in HAVA. *See, e.g.*, 42 U.S.C. § 15329:

> The [Election Assistance] Commission shall not have any authority to issue any rule, promulgate any regulation, or take any other action which imposes any requirement on any State or unit of local government, except to the extent permitted under section 9(a) of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-7(a)).

See also 42 U.S.C. § 15485:

> The specific choices on the methods of complying with the requirements of this title [Title III, entitled "Uniform and Nondiscriminatory Election Technology and Administration Requirements"] shall be left to the discretion of the states.

Importantly, while state discretion is permitted in determining how to comply, HAVA nevertheless compels states to comply with the specified minimum standard and functions. The nationwide empirical record abundantly evinces technological noncompliance of voting systems.

81. *See* 42 U.S.C. § 15329, which provides:

> The Commission shall not have any authority to issue any rule, promulgate any regulation, or take any other action which imposes any requirement on any State or unit of local government, except to the extent permitted under section 9(a) of the National Voter Registration Act of 1993 (42 U.S.C. § 1973gg-7(a)).

82. *See Voting and Registration Technology Issues*, *supra* note 9.

83. *See* HAVA, 42 U.S.C. § 15361.

84. 42 U.S.C. §§ 15482(a)(2), (5). Unfortunately, no judicial or media records evidence any Department of Justice effort to enforce these auditability and accuracy provisions, other than the lawsuit against New York for failure to replace its lever systems. United States v. New York, No. 06-CV-0263, 2006 U.S. Dist. LEXIS 27664 (N.D.N.Y. May 9, 2006) (denying reconsideration of denial to intervene) (unreported). This case eventually settled.

85. The National Association of State Election Directors (NASED) created and administered with the Election Center's assistance a lab certification program for testing voting systems for "qualification"—compliance with the FEC standards. The term "qualified" was used, 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 included the FEC standards. *See* Stephanie Philips, *The Risks of Computerized Election Fraud: When Will Congress Rectify a 38-Year-Old Problem?*, 57 ALA. L. REV. 1123 (2006). Once a voting system passed qualification testing, it was assigned a "Qualification Number" and no further qualification tests were performed unless modifications were made to the voting systems by vendors. *See* Federal Election Commission, *Voting Systems Performance and Test Standards: An Overview* 1 (Agenda Dec. 13, 2001) ("Since NASED's testing program was initiated in 1994, more than 30 voting systems or components of voting systems have gone through the NASED testing and qualification process. In addition, many systems have subsequently been certified at the state level . . . .") http://www.fec.gov/agenda/agendas2001/mtgdoc01-62/overview.htm (last visited Mar. 7, 2012) [hereinafter *FEC Overview*].

86. Before HAVA, in the absence of explicit statutory authority, the FEC had attempted to redress the regulatory vacuum by developing and issuing voting system standards, but few resources and little authority had been authorized. *See* SALTMAN, *supra* note 1, at 169–74, 179–85. The FEC commented, "As the qualification process matured and as qualified systems were used in the field, the [FEC] Voting Systems Board . . . was able to identify certain testing issues that needed to be resolved. Moreover, rapid advancements in information and personal computer technologies have introduced new voting system development and implementation scenarios not contemplated by the 1990 Standards." *FEC Overview*, *supra* note 85.

87. FEC, *History of the Voting System Standards Program*, http://www.fec.gov/pages/vsshst.htm.

88. *See* BROKEN BALLOTS, *supra* note 1; Doug Jones, *Problems with Voting Systems and the Applicable Standards*, Testimony before the H.R. Comm. on Science, Washington, D.C. (May 22, 2001), http://www.divms.uiowa.edu/~jones/voting/congress.html. *See, e.g.*, JOHN FUND, STEALING ELECTIONS 1–9 (2004); Richard L. Hasen, *Beyond the Margin of Litigation: Reforming U.S. Election Administration to Avoid Electoral Meltdown*, 62 WASH. & LEE L. REV. 937, 942 (2005); Philips, *supra* note 85, at 1123–50.

89. *See* BROKEN BALLOTS, *supra* note 1, at 139–41.

90. *See* GAO, *Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed*, GAO-05-956, at 43–45 (Sept. 2005), http://www.gao.gov/assets/250/247851.pdf (noting that "TGDC and NIST have been working on behalf of EAC to improve the 2002 Federal Election Commission voluntary voting system standards and their impact on the acquisition, testing, operations, and management processes

of the voting system life cycle"). The FEC 2002 standards were issued while HAVA was drafted, with recognition that HAVA articulated a new collaborative structure for updating the FEC's interim effort. The GAO continued, "TGDC's initial priorities have been to correct errors and fill gaps in the 2002 standards and to supplement them with provisions that address HAVA requirements." *Id.* at 45.

91. *See, e.g.*, Avi Rubin, *The Dirty Little Secrets of Voting System Testing Labs*, http://www.huffingtonpost.com/avi-rubin/the-dirty-little-secrets-_b_12354.html; *see also* two TTBR assessments that included review of the confidential testing lab reports: CANDICE HOKE & DAVE KETTYLE, DOCUMENTATION ASSESSMENT OF THE DIEBOLD VOTING SYSTEMS 2 (TTBR 2007), http://www.sos.ca.gov/voting-systems/oversight/ttbr/diebold-doc-final.pdf (commenting that the lab report of 16 pages was too brief and presented insufficient "detail on the methodologies, tests, or results that were obtained"; the report thus does "not permit a reader to formulate an informed opinion on the degree to which the Diebold voting system met or exceeded the minimum federal standards for qualification"; JOSEPH LORENZO HALL & LAURA QUILTER, DOCUMENTATION REVIEW OF THE HART INTERCIVIC SYSTEM 6.2.1 VOTING SYSTEM 24–31, 64 (2007), http://www.sos.ca.gov/voting-systems/oversight/ttbr/hart-doc-final.pdf (noting that "the poorly documented testing reports and the complete lack of detailed test plans . . . put state-level certification at an information disadvantage by largely fail[ing] to communicate information [needed] to assess the systems" with respect to compliance with FEC 2002 Voting System Standards).

92. Whether HAVA supplies a private right of action to enforce some of its provisions remains an open question. In *Ohio Republican Party v. Brunner*, 555 U.S. 5 (2008), the U.S. Supreme Court intimated a negative but did not directly decide this question. *See* Daniel Tokaji, *Public Rights and Private Rights of Action: The Enforcement of Federal Election Laws*, 44 IND. L. REV. 113 (2010) (arguing for private rights of action under HAVA).

93. By contrast, the Department of Justice has sought to enforce HAVA's physical accessibility and multiple language requirements and certain National Voter Registration Act (NVRA) requirements via litigation. The Department's webpage presents information on recent election and voting rights statutory enforcement, http://www.justice.gov/crt/about/vot/whatsnew.php, specifically discussing several cases the Department has settled; these include *United States v. Alameda County, California* (language), *United States v. Lorain County* (Puerto Rican bilingual voting rights), and *United States v. Louisiana* (NVRA). *See also* ELECTIONLINE.ORG at 7–8 (2007).

94. A relatively comprehensive inventory of scientific studies of voting systems through 2008 with links to their public reports can be found in MATT BISHOP, MARK GRAFF, CANDICE HOKE, DAVID JEFFERSON & SEAN PEISERT, RESOLVING THE UNEXPECTED IN ELECTIONS: ELECTION OFFICIALS' OPTIONS, Appendix 2: Voting Systems Studies 22–27 (2008), *available at* http://nob.cs.ucdavis.edu/bishop/notes/2008-forensic/index.html (providing a guide to indicators of possible electronic malfunctions and forensic assessments to determine whether the tabulation reports deserve trust). Virtually all reports include an Executive Summary written in language accessible for the lay audience. The TTBR covers many of the current voting systems deployed nationwide in 2012. The other set of comprehensive scientific assessments, Project

EVEREST, has links posted on the Pennsylvania State University website, http://siis.cse.psu.edu/everest.html (last visited Feb. 11, 2012). *See supra* note 9 (discussing TTBR and EVEREST reports). *See also Written Testimony of David Wagner, Ph.D.: Hearing Before the Comm. on Science and Comm. on House Administration*, 109th Cong. 2 (July 19, 2006) (statement of David Wagner, Ph.D., Computer Science professor, University of California, Berkeley).

95. The field performance record of currently deployed voting technologies is reviewed more extensively in *Voting and Registration Technology Issues*, *supra* note 9, and citations therein. Consider also the comment of New York State Board of Elections Co-Chair Douglas Kellner, who summarized the situation at a Board meeting: "the voting industry sells crap, and that is the problem . . . ." Rady Ananda, *NY Loves Its Levers as New Voting Systems Fail*, http://www.opednews.com/articles/NY-Loves-Its-Levers-as-New-by-Rady-Ananda-080701-173.html. Florida's Secretary of State Kurt Browning testified before the EAC:

> [V]endors will hear about [this] when we meet next month, but I do not understand, I cannot fathom how you can produce automobiles, you can produce airplanes, you can produce washing machines, you can produce refrigerators, name the product, and you know that when you plug it in it's going to work. But with voting systems, there's just something systemically wrong that the products that are coming off the line are not dependable.
>
> My goal in Florida, is that when we open the polls in 2010, that we have a very high level of confidence that when those Supervisors of Elections in the county plug those things in and turn them on it's like turning on your TV. We don't have to hold our breath to see if those things are going to come up . . . .

Minutes of the Public Meeting, U.S. Election Assistance 106 (Dec. 8, 2008), http://www.eac.gov/assets/1/AssetManager/transcript%20public%20meeting%20december%208%2020081.pdf (discussing the poor reliability of voting systems).

96. *See, e.g.*, Ariel J. Feldman, J. Alex Halderman & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine* (2007), https://www.usenix.org/conference/evt-07/security-analysis-diebold-accuvote-ts-voting-machine.

97. For example, TTBR scientists explained their findings:

> The . . . teams demonstrated that the security mechanisms provided for all systems analyzed were *inadequate to ensure accuracy and integrity of the election results* and of the systems that provide those results.

Matt Bishop, *Overview of the Red Team Reports [covering Sequoia, Diebold/Premier, and Hart Intercivic voting systems brands]* 11, http://www.sos.ca.gov/voting-systems/oversight/ttbr/red-overview.pdf (emphasis added). Other TTBR scientists who evaluated the source code for one system summarized their conclusion that applies to the other vendors as well:

> [T]he technological controls in the Diebold software *do not provide sufficient security to guarantee a trustworthy election*. The software contains serious design flaws that have led directly to specific vulnerabilities that attackers could exploit to affect election outcomes. These vulnerabilities include:

> **Vulnerability to malicious software**
>
> The Diebold software contains vulnerabilities that could allow an attacker to install malicious software on voting machines or on the election management system. Malicious software could *cause votes to be recorded incorrectly or to be miscounted, possibly altering election results*. It could also prevent voting machines from accepting votes, potentially causing long lines or *disenfranchising voters*.

Joseph A. Calandrino et al., *Source Code Review of the Diebold Voting System* at i (July 20, 2007), *available at* http://www.sos.ca.gov/voting-systems/oversight/ttbr/diebold-source-public-jul29.pdf (emphasis added); *see also CWE/SANS TOP 25 Most Dangerous Software Errors*, http://cwe.mitre.org/top25/.

The United States has made cyber security improvement a major focus and is now extending its efforts into reporting on vulnerabilities in election software. The Common Weakness Enumeration (CWE) is a federally funded software assurance project designed to help upgrade the software industry's persistent neglect of easily exploited yet avoidable vectors for remote hacking by identifying the most pervasive and dangerous avoidable coding errors. Neither higher educational programs in computer science nor the industry has placed high priority on knowledge and coding skills that achieve security. The economic, personal, and national security consequences are extraordinary. *See* DAVID RICE, GEEKONOMICS: THE REAL COST OF INSECURE SOFTWARE *passim* (2007); Tim Green, *"Rugged Manifesto" Promotes Secure Coding; Goal Is to Raise Awareness of Pitfalls and Adherence to Sound Programming Principles*, NETWORK WORLD (Feb. 8, 2010), http://www.networkworld.com/news/2010/020810-rugged-manifesto-secure-coding.html (last visited Mar. 5, 2012) (reporting on rationale of new software security effort: "The problem . . . is that developers write code assuming the only task is to make it perform a function. But that can lead to programs riddled with vulnerabilities that can in turn lead to economic damages, lost data and lost productivity . . . [quoting *Rugged* co-founder Corman] 'We have to get to the mass of programmers who simply don't realize their code is being attacked and subverted by talented and persistent adversaries.'"). Part of the U.S. national security effort is dedicated to upgrading security of information systems in measurable ways. *See generally* MAKING SECURITY MEASURABLE, http://measurablesecurity.mitre.org/about/index.html, and the Department of Homeland Security's (DHS) BUILD SECURITY IN website, https://buildsecurityin.us-cert.gov/bsi/home.html ("Build Security In is a collaborative effort that provides practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development."). DHS and its contractor MITRE Corporation have generated voting systems security models that reveal the serious vulnerabilities of the deployed systems. *See* CWRAF Domains, Technology Groups, Archetypes, and Vignettes, http://cwe.mitre.org/cwraf/vignettes.html#evoting-Internet (last visited Apr. 28, 2012).

98. Scientists have examined other nations' electronic voting systems' security and accuracy, documenting serious flaws. For instance, insufficient security design can compromise vote accuracy and machine availability to voters. *See, e.g.*, Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati & Rop Gonggrijp, *Security Analysis of India's Electronic Voting Machines*, Proc. 17th ACM Conference on Computer and Communications Security (CCS '10), Chicago (Oct. 2010), and http://indiaevm.org/ (video presentation).

99. Precinct-based optical scanners do provide the combination of a voter-created paper record for recounts and checks on the software tabulations, so they are a far better option than DREs.

100. The EAC voting system certification webpage lists some newer voting equipment currently undergoing federal certification assessments that has not been subjected to the independent testing conducted under the TTBR and EVEREST. *See supra* note 22.

101. Douglas W. Jones, *Counting Mark-Sense Ballots: Relating Technology, the Law and Common Sense*, Douglas W. Jones on Voting and Elections, http://www.divms.uiowa.edu/~jones/voting/optical/ (last visited Feb. 12, 2012) (quoting James Baker, as quoted by CNN on Nov. 12, 2000).

102. Touchston v. McDermott, 234 F.3d 1161 (11th Cir. 2000) (emphasis added).

103. Jones, *supra* note 101; *see also* Jones, *supra* notes 88 and 63.

104. *See supra* note 58 (discussing Paul M. Schwartz, *Voting Technology and Democracy*).

105. Each of these points is more extensively developed in *Voting and Registration Technology Issues*, *supra* note 9. *See also* H.R. Rep. No. 672 (2011) (seeking to terminate the EAC and transfer its functions), explained at http://cha.house.gov/bill/bill-terminate-election-assistance-commission.

106. The NASS resolutions can be found at http://www.nass.org/index.php?option=com_content&view=article&id=87&Itemid=386.

107. *See, e.g.*, Opening Statement of Senator Lamar Alexander, U.S. Senate Committee on Rules and Administration, http://rules.senate.gov/public/?a=Files.Serve&File_id=411fc971-c493-4c27-b99e-2aa653cf6120=2011 (June 29, 2011) (detailing reasons for terminating the EAC). *See also* H. Comm. on Administration, Markup of H.R. 672, http://cha.house.gov/markup/markup-hr-672-hr-1934-committee-resolution-112-8 (amending HAVA to terminate the EAC and transfer its powers).

108. *See NASS Resolution on the Continued Functioning of the EAC Standards Board and Board of Advisors*, http://www.nass.org/index.php?option=com_content&view=article&id=87&Itemid=386 (passed Jan. 31, 2012).

109. *See generally* EAC, State Requirements and the Federal Voting System Testing and Certification Program, http://www.eac.gov/assets/1/Page/State%20Requirements%20and%20the%20Federal%20Voting%20System%20Testing%20and%20Certification%20Program.pdf.

110. *See generally Voting and Registration Technology Issues*, *supra* note 9, at 43–45.

111. *See* Letter from EAC to Registered Manufacturer [of Voting Systems] (June 27, 2011), *at* http://www.eac.gov/assets/1/Documents/Program_Drector_Letter_to_Manufacturers_re_Readiness_for_Testing_6%2027%2011.pdf (last visited Mar. 12, 2012) ("Over the course of the last 12–18 months, the EAC has noticed what appears to be an increasing trend in which voting systems submitted to the EAC for conformance testing to the VVSG [voting system standards] are clearly not ready to be tested by our VSTLs. Recent examples include . . . submission of software packages containing numerous fundamental coding discrepancies. Submitting systems for testing before they are functionally ready . . . is a waste of time and money for all entities involved in this process. The EAC reminds manufacturers that VSTL testing should not be used to replace rigorous internal pre-production and beta testing by voting system manufacturers.").

112. *Compare* Remarks of David Beirne, Executive Director of the [voting system vendors' trade group] Election Technology Council, to the Joint Election Official Liaison Committee (Jan. 8, 2009) (urging the election officials to "embrace the principle of testable performance requirements, not design specifications, for voting system standards") *with* Earl Barr, Matt Bishop & Mark Gondree, *Fixing Federal E-Voting Standards*, COMMUNICATIONS OF THE ACM, Mar. 2007, at 19, 24 ("Neither the government nor electronic voting system vendors have adequately addressed these design and certification flaws, let alone advanced solutions"; also: "We need to move beyond the 'patch' approach to electronic voting systems, using high-assurance techniques to design and implement systems that provide the requisite guarantees."). Note that election officials have no expertise in development methods for designing information systems that can achieve high standards of accuracy and reliability, or other technical attributes, but do have important experience relevant for usability engineering. While it may appear "reasonable" for Beirne and the vendors to request that federal voting systems guidelines be limited to performance standards, that position does not evince an understanding of the software industry's development process for contexts demanding high accuracy and security, or even its normal information systems software development process. *See* GAO, *Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed*, GAO-05-956 (Sept. 2005), http://www.gao.gov/assets/250/247851.pdf (reviewing the life cycle of voting systems as an information system: "The product development phase includes activities such as establishing requirements for the system, designing a system architecture, and developing software and integrating components. . . . Design and development activities related to security and reliability of electronic voting systems include such things as requirements development and hardware and software design"). The trade group's more extensive document, Election Technology Council (ETC), BROKEN: THE REGULATORY PROCESS FOR THE VOTING INDUSTRY (2008), urges changes to the regulatory system contrary to best practices for software development. The ETC issued this report after its executive director Beirne and this author served on a panel on voting technology (at the Pew Charitable Trusts media event in Chicago, December 2007). This author argued that the then-current HAVA voting system regulatory structure had not been well designed to achieve high-quality software, and that it did not well serve any constituency, including the equipment vendors. While this argument advanced marketing and public advantages for high-quality, secure voting software, ETC's response in BROKEN suggests a *de minimis* regulatory and testing lab structure.

113. *See, e.g.*, League of Women Voters of Ohio v. Brunner, 548 F.3d 463 (6th Cir. 2008) (ruling in favor of plaintiffs claiming that the election administrative system systematically deprived Ohio voters of their equal protection rights); Chavez v. Brewer, 214 P.3d 397 (Ariz. 2006) (challenging the voting systems under the Fourteenth Amendment and the Voting Rights Act); Conroy v. Dennis, No. 06-CV-6072 (Colo. Oct. 19, 2006) (unpublished), *available at* http://www.wtotrial.com/conroy-v-dennis-colorado-secretary-of-state-no-06-cv-6072-colo-oct-19-0 (claiming that DRE systems were illegal under Colorado state law); Stewart v. Blackwell, 444 F.3d 843 (6th Cir. 2006) (challenging voting systems under the Fourteenth Amendment and the Voting Rights Act); Weber v. Shelley, 347 F.3d 1101 (9th Cir. 2003) (contending that equal protection was violated by some voters' inability to cast ballots

on voting systems with paper audit trail); Black v. McGuffage, 209 F. Supp. 2d 889 (N.D. Ill. 2002) (alleging that differential undervote rate deprived minority voters of franchise rights protected by the Equal Protection Clause).

114. For example, the Arizona Legislature amended and enacted several statutes to effectuate HAVA. Among these changes, the legislature amended Arizona Revised Statutes (A.R.S.) Section 16-442(A) to require that the Secretary of State determine the voting machines that are "certified for use" in elections. 2003 ARIZ. SESS. LAWS ch. 260, § 9 (1st Reg. Sess.). Florida amended its recount laws and also began the process of evaluating voting technologies to replace the punch-card system.

115. *See* Carrington v. Rash, 380 U.S. 89, 96 (1965) (stressing that "free and honest elections are the very foundation of our republican form of government").

116. Other factors could include size of jurisdiction, ease of use by elderly voters, and costs of maintenance over time. The states would retain discretion to weigh factors not legally barred.

117. *See* Heather K. Gerken, *Election Law Exceptionalism: A Bird's Eye View of the Symposium*, 737 B.U. L. REV. 743–44 (2002).

118. Many leading scholars of election law perceive the need to transform the paradigm from an individual rights framework to a structural analysis. *See, e.g.*, Heather K. Gerken, *Understanding the Right to an Undiluted Vote*, 114 HARV. L. REV. 1663 (2001) (maintaining that vote-dilution claims cannot fit comfortably within the conventional individual-rights framework that the Court tends to use); Richard H. Pildes, *The Theory of Political Competition*, 85 VA. L. REV. 1605, 1611 (1999) (recommending a structural approach because the "constitutional values of American democracy" depend on "appropriately competitive interorganizational conditions"); Lani Guinier, *[E]racing Democracy: The Voting Rights Cases*, 108 HARV. L. REV. 109 (1994) (arguing against the adequacy of existing voting rights jurisprudence for handling racial groups' claims); Laurence H. Tribe, *Saenz Sans Prophecy: Does the Privileges or Immunities Revival Portend the Future—Or Reveal the Structure of the Present?*, 113 HARV. L. REV. 110, 159–60, 170–72 (1999) (demonstrating that the Supreme Court forgoes structural analysis when deciding civil-rights and equal-protection claims); Daniel R. Ortiz, *From Rights to Arrangements*, 32 LOY. L.A. L. REV. 1217, 1218 (1999) (observing the movement of election law scholarship "away from a largely rights-based, individual-centered view of politics, to a more pragmatic and structural view of politics"); Samuel Issacharoff & Richard H. Pildes, *Politics as Markets: Partisan Lockups of the Democratic Process*, 50 STAN. L. REV. 643 (1998) (suggesting that courts should approach voting claims in structural terms).

119. Premier Election Solutions, Inc. filed against the Cuyahoga County Board of Elections and the state of Ohio in Franklin County courts for a declaratory judgment that it had fulfilled its legal obligations. No reported decision is available but the case eventually settled. *See* K.C. Jones, *Electronic Voting Machines at Center of Ohio Lawsuits*, INFO. WK. (Aug. 8, 2008), http://www.informationweek.com/news/global-cio/legal/210000402.

120. *Id.*

121. The Ohio Secretary of State's response is detailed in a press release, *Ohio Secretary of State Files Counterclaim in Lawsuit with Premier Election Solutions*, http://www.votetrustusa.org/index.php?option=com_content&task=view&id=2926&Itemid=51.

122. Steve Rosenfeld, *San Francisco Seeks Multi-Million Dollar Voting Machine Refund*, http://www.alternet.org/story/67370/san_francisco_seeks_multi-million_dollar_voting_machine_refund/.

123. Montgomery Cnty. v. Microvote Corp., 175 F.3d 296 (3d Cir. 1999).

124. 42 U.S.C. § 1973(a) (codifying § 2); 42 U.S.C. § 1973(c) (codifying § 5).

125. *See* City of Boerne v. Flores, 117 S. Ct. 2157 (1997); Daniel P. Tokaji, *The New Vote Denial: Where Election Reform Meets the Voting Rights Act*, 82 S.C. L. Rev. 689, 691–92 (2006); Black v. McGuffage, 209 F. Supp. 2d 889 (N.D. Ill. 2002) (alleging that differential undervote rate deprived minority voters of franchise rights protected by the Equal Protection Clause).

126. Tokaji, *supra* note 125. Professor Pamela Karlan explains the Voting Rights Act "two-step" in *Two Section Twos and Two Section Fives: Voting Rights and Remedies After* Flores, 39 Wm. & Mary L. Rev. 725 (1998).

127. Tokaji, *supra* note 125. *Shelby County, Alabama v. Holder*, No. 11-5256, pending in the D.C. Circuit, is one of several lawsuits seeking to invalidate Section 5 as unconstitutionally burdensome.

128. Stewart v. Blackwell, 444 F.3d 843 (6th Cir. 2006), *vacated as moot*, 473 F.3d 692 (6th Cir. 2007) (challenging Ohio's maintenance of different types of voting technologies that produced different error rates and risk of vote loss; court held that voters had an unequal chance of having their votes counted, in violation of the Equal Protection Clause).

129. In *League of Women Voters of Ohio v. Brunner*, 548 F.3d 463 (6th Cir. 2008), the League challenged Ohio's election administration system as constituting structural violations against the voting public. The case settled with a consent decree. *See* Lawyers Committee for Civil Rights Under Law (explanatory note with case document links) *at* http://www.lawyerscommittee.org/projects/voting_rights/page?id=0048.

130. *Ohio League* presented two crucial Fourteenth Amendment issues that in the post-*Bush* era have led to a divergence among the circuits: the appropriate standard of review and whether the claim requires proof of intent to discriminate. The Sixth Circuit reasoned:

> The Secretary and Governor argued in the district court, and before us, that the equal protection claim requires a showing of "intentional and purposeful discrimination." The League contends that the proper scienter requirement is, alternatively, knowledge, willful blindness, or deliberate indifference. We need not decide this issue, however, because *the only question before us is whether the amended complaint pleads facts, if proven, sufficient to establish that the defendants arbitrarily deny Ohioans the right to vote depending on where they live.*

League of Women Voters of Ohio v. Brunner, 548 F.3d at 476 (citations omitted) (emphasis added). *See* Bush v. Gore, 531 U.S. 98, 104–05 (2000) (*per curiam*) ("Having once granted the right to vote on equal terms, the State may not, by later *arbitrary and disparate* treatment, value one person's vote over that of another.") (emphasis added); Reynolds v. Sims, 377 U.S. 533, 557 (1964) (noting that "arbitrary and capricious action" can violate the Fourteenth Amendment) (quoting Baker v. Carr, 369 U.S. 186, 226 (1962)).

In *Hunter v. Hamilton County Board of Elections*, 635 F.3d 219, 234 (6th Cir. 2011), the standard of review and scienter issues resurfaced with largely the same resolution. The court relied on Professor Ned Foley's analytic approach in reaching its decision. *See* Edward B. Foley, *Refining the* Bush v. Gore *Taxonomy*, 68 Ohio St. L. Rev. 1035, 1037 (2007). On remand, *Hunter v. Hamilton County Board of Elections*, 2012 WL 404786 (S.D. Ohio Feb. 8, 2012), the court ruled that the Board had not complied with requirements of the Equal Protection Clause in determining which provisional ballots it would count.

131. The plaintiffs summarized the settlement's voting technology and security provisions:

> Improvements to be maintained in the area of voting technology and security include procedures for post-election audits of ballots; procedures requiring paper ballots in event of DRE machine breakdown; statewide standards for Logic and Accuracy testing of tabulating machines, statewide standards for VVPAT quality and handling; security procedures for components of voting systems; and statewide standards on physical security of voting equipment.

The Lawyers' Committee for Civil Rights Under Law, *What LWVO v Brunner Settlement Means for Ohio Voters, available at* http://www.lawyerscommittee.org/projects/voting_rights/page?id=0046 (last visited May 10, 2012).

132. Black v. McGuffage, 209 F. Supp. 2d 889 (N.D. Ill. 2002) (alleging that differential undervote rate deprived minority voters of franchise rights protected by the Equal Protection Clause); *see also* Sw. Voter Registration & Educ. Project v. Shelley, 344 F.3d 882, *rev'd en banc*, 344 F.3d 914 (9th Cir. 2003) (overturning the panel's enjoining of the special election owing to alleged voting technology (punch-card) deficiencies).

133. League of Women Voters of Ohio v. Brunner, 548 F.3d at 466, 470 (emphasis added) (citations omitted).

134. Professors Heather Gerken and Spencer Overton are among those election law scholars who have developed the structural analysis. *See* Heather K. Gerken, *Understanding the Right to an Undiluted Vote*, 114 Harv. L. Rev. 1663, 1681–91 (2001) (discussing the concept of "aggregate rights" for vote-dilution claims); Spencer Overton, *A Place at the Table:* Bush v. Gore *Through the Lens of Race*, 29 Fla. St. U. L. Rev. 469, 490 (2001) ("Many Americans of various backgrounds . . . use voting as a means to maintain communities of identity and to exert collective self-determination in shaping their world through the political process.").

135. For further development of this argument, *see* Candice Hoke, *Judicial Protection of Popular Sovereignty: Redressing Voting Technology*, Case W. L. Rev. (Symposium; forthcoming summer 2012). The structural aspects of voting technology and the Equal Protection Clause's promise of equality in the likelihood that the vote will be counted accurately as cast have led some commentators to argue for a unitary, statewide voting system. *See, e.g.*, Stewart v. Blackwell, *Punch Card Ballots v. Direct Record Electronic Voting: Why Ohio's Use of Different Methods to Count Ballots Violates the Equal Protection Clause*, 31 U. Dayton L. Rev. 527 (2006). While on its face one statewide voting system appears feasible and compliant with the Fourteenth Amendment, computer security teaches us that unless the unitary system has been developed using high assurance techniques, it poses substantially greater risks to accurate election counts and to the overall availability and reliability of the voting system than do multiple systems. The impact of coding errors would be magnified, and the value of working on a successful exploit would be much higher. Without substantial additional security safeguards

in place, such as robust post-election auditing of results, the unitary voting system does not supply an acceptable answer to the equal-protection quest.

136. Andrade v. NAACP of Austin, 345 S.W.3d 1 (Tex. 2011) (ruling that state law committed the choice of voting technology to the Secretary of State, and thus the court would not reassess her decisions).

137. John Hart Ely has warned of the possibilities of a "political lockup." In Ely's view, our government can be said to be "malfunctioning" when "the ins are choking off the channels of political change to ensure that they will stay in and the outs will stay out." John Hart Ely, Democracy and Distrust: A Theory of Judicial Review 103 (1980). When such behavior occurs, Ely argues, "the process is undeserving of trust." He calls for not only judicial action to prevent outright "denial of the vote," but also "[o]ther practices that go to the core of the right of the people to choose their representatives." *Id.* Ely influenced Paul Schwartz's emphasis of the importance of robust judicial policing of the political branches' choices and management of voting technology. *See* Paul M. Schwartz, *Voting Technology and Democracy,* 77 N.Y.U. L. Rev. 625, 678–97 (2002).

138. Gusciora v. Christie, Appellate Docket No. A-005608-10T3; Gusciora v. McGreevey, 395 N.J. Super. 422 (App. Div. 2006). For an assessment of the value of tamper-evident security seals for protecting voting systems' integrity, see the article by plaintiffs' expert witness Professor Andrew Appel, *Security Seals on Voting Machines: A Case Study,* ACM Transactions on Information and System Security (TISSEC) (2011), http://www.cs.princeton.edu/%7Eappel/voting/SealsOnVotingMachines.pdf.

139. *See supra* text accompanying notes 38–42.

140. Banfield v. Cortes (*substituted* Aichele), 922 A.2d 36 (Pa. Commw. Ct. 2007) (permitting the case to move into discovery).

141. *See* DOJ, Civil Rights Division, Voting Section, http://www.justice.gov/crt/about/vot/whatsnew.php.

142. *Id.* These standards are found in § 301 of Title III, *codified at* 42 U.S.C. § 15481.

143. Part of the Civil Rights Act of 1960, 42 U.S.C. § 1974, mandates the retention and preservation of records concerning federal elections:

> Every officer of election shall retain and preserve, for a period of twenty-two months from the date of any . . . election of which candidates for . . . [federal office] are voted for, all records and papers which come into his possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election.

144. Part of HAVA § 301, codified at 42 U.S.C. § 15481(a)(5), addresses voting systems tabulations by specifying the permissible error rate and hence the accuracy rate required of voting systems used in federal elections:

> *The error rate of the voting system in counting ballots* (determined by taking into account only those errors which are attributable to the voting system and not attributable to an act of the voter) *shall comply with the error rate standards* established under section 3.2.1 of the voting systems standards issued by the Federal Election Commission which are in effect on October 29, 2002.

(Emphasis added.) Although compliance with the original FEC error rate was assessed during laboratory compliance testing, that aspect was not codified as part of HAVA. Significant empirical evidence exists that the voting systems have amassed field error rates of 8–10 percent of all ballots, not of only "ballot positions" or choices possible, outstripping the FEC error rate by a factor of over 10 times. Arguably, a voting system that cannot maintain a low error rate in actual elections is of far greater relevance to voting rights than is the rate in a lab certification test, and is of constitutional dimension.

145. Observing the DOJ's nonenforcement of the standards is not to suggest that the HAVA standards are well designed or sufficiently specific to protect voting rights. *See* Broken Ballots, *supra* note 1, at 139–41. But they are statutory minimums and yet have still been neglected by the primary entity that HAVA charged with their enforcement.

146. In one enforcement action relating to enforcement of the "notice" voting protections specified in 42 U.S.C. § 15481, the DOJ sued the New York State Board of Elections (SBOE) for not undertaking the required rapid transition to notice or e-voting; only peripheral motions resulted in judicial records as the case settled. *See* United States v. N.Y. State Bd. of Elections, 312 F. App'x 353; 2008 U.S. App. LEXIS 8099 (2d Cir. 2008) (denial of intervention affirmed); United States v. New York, No. 06-CV-0263, 2006 U.S. Dist. LEXIS 27664 (N.D.N.Y. May 9, 2006) (denying reconsideration of denial to intervene). The New York SBOE contended that its first responsibility was to ensure that New Yorkers' state constitutional rights to vote were realized. Second, the Board claimed that none of the available technology had been engineered to attain the levels of accuracy and security required by the New York Constitution for voting rights protection. The settlement required New York to move forward into purchasing and deploying electronic voting systems despite their deficiencies, but New York has established a more robust internal testing apparatus to identify flaws and require remediation before deployment.

147. HAVA's auditability section, 42 U.S.C. § 15481(a)(2), provides:

> (2) Audit Capacity
>
> (A) In General—The voting system shall produce a record with an audit capacity for such system.
>
> (B) Manual Audit Capacity
>
> (i) The voting system shall produce a permanent paper record with a manual audit capacity for such system.
>
> (ii) The voting system shall provide the voter with an opportunity to change the ballot or correct any error before the permanent paper record is produced.
>
> (iii) The paper record produced under subparagraph (A) shall be available as an official record for any recount conducted with respect to any election in which the system is used.

148. *See, e.g.*, Gray v. Sanders, 372 U.S. 368, 380 (1963), and textual discussion.

149. *Id.*

150. 377 U.S. 533, 554–55 (1964) (internal quotation marks and citations omitted).

151. *Id.* "The right to vote can neither be denied outright, nor destroyed by alteration of ballots, nor diluted by ballot-box stuffing." *Id.* at 555 (citations omitted). The Court also quoted *United States v. Classic,* 313 U.S. 299, 315 (1941): "Obviously included within the right to choose, secured by the Constitution, is the right of qualified voters within a state to cast their ballots and have them counted . . . ."

152. Ohio Republican Party v. Brunner, 555 U.S. 5 (2008).

153. 42 U.S.C. § 15511 (for enforcement of Title III, §§ 301, 302, and 303).

154. Baker v. Carr, 369 U.S. 186 (1962).

155. Reynolds v. Sims, 377 U.S 533 (1964) (holding the Alabama legislative plan for redistricting the legislature invalid under the Equal Protection Clause). The *Reynolds* Court's language has been repeatedly quoted and provides the touchstone for many decisions adjudicating burdens on voting rights:

> Undoubtedly, the right of suffrage is a fundamental matter in a free and democratic society. Especially since *the right to exercise the franchise in a free and unimpaired manner is preservative of other basic civil and political rights,* any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized. Almost a century ago, in *Yick Wo v. Hopkins,* the Court referred to "the political franchise of voting" as *"a fundamental political right, because preservative of all rights."*

Id. at 561–62 (internal citations omitted) (emphasis added).

156. As Paul Schwartz has observed, "we have seen how the unequal distribution of voting technology in Florida correlated with disparities of race and wealth. . . . There has in fact been a long tradition in the United States of designing election systems to block access to the franchise by racial minorities and the poor." Paul M. Schwartz, *Voting Technology and Democracy,* 77 N.Y.U. L. Rev. 625, 675–79 (2002) (explaining how political "lockups" of the politically powerful can be achieved and perpetuated via voting system designs that are not properly policed judicially). The perspicacity of this insight may be seen in current voting systems with design features that permit covert tampering (and software bugs) to negate voters' authentic selections and additionally that allow untraceable destruction of evidence by erasing logging of the activity, or by configuring logs to not record activity, arguably violating 42 U.S.C. § 1974. *See also* Yasmin Dawood, *The Antidomination Model and the Judicial Oversight of Democracy,* 96 Geo. L.J. 1411 (2008) (theorizing the political lockup model).

157. *See infra* text accompanying notes 162–163.

158. HAVA delegates enforcement power in 42 U.S.C. § 15511 for enforcement of Title III, §§ 301, 302, and 303, providing that the Attorney General

> may bring a civil action against any State or jurisdiction in an appropriate United States District Court for such declaratory and injunctive relief (including a temporary restraining order, a permanent or temporary injunction, or other order) as may be necessary to carry out the uniform and nondiscriminatory election technology and administration requirements under [Section 301 of HAVA.]

But DOJ also has more sweeping enforcement powers under the Voting Rights Act, the Civil Rights Acts (including Section 1983), and a broad array of election criminal statutes. Because computer-based voting systems are the mechanism by which votes are recorded, tabulated, and reported, DOJ must develop technical voting systems background in order to fulfill its duties under all its statutory delegations regarding voting rights protection.

159. U.S. Const. amend. 14, § 1. The Sixth Circuit ruled that the *Ohio League* complaint had properly stated a substantive due process claim related to voting system operation and governmental management. *See* League of Women Voters of Ohio v. Brunner, 548 F.3d 463, 478 (6th Cir. 2008).

160. This author, however, would not agree that DOJ is the only proper plaintiff to bring HAVA enforcement actions under 42 U.S.C. § 15511. All the HAVA provisions authorizing DOJ enforcement are grouped under Title III, with the descriptive name "Uniform and *Nondiscriminatory* Election Technology and Administration Requirements." *See* HAVA, 42 U.S.C. § 15481 (emphasis added). This language evinces a crucial congressional understanding that the choice of particular voting technologies and their technical specifications that relate to accuracy and auditability—whose reliable realization will in turn depend in part on security design and implementation—are integral components of the right to vote. Additionally, enforcement of federal civil-rights statutes is rarely vested exclusively in government actors. DOJ's decade of nonenforcement of HAVA's provisions addressing technical accuracy and security specifications lends substantial support to the need for private-party enforcement, as per *Cannon v. University of Chicago*, 441 U.S. 677, 708 n.42 (1979) (authorizing an implied private remedy to enforce Title IX, as helping to overcome impediment of limited federal fiscal resources to full enforcement). *See also* Daniel P. Tokaji, *Public Rights and Private Rights of Action: The Enforcement of Federal Election Laws*, 44 Ind. L. Rev. 113, 114–15 (2010) (arguing that the Court's doctrinal criteria for implying a private right of action do not account for the essential supervisory role of the federal courts in protecting franchise right and structural prerequisites of fair elections especially in pre-election litigation; criteria would defeat courts' roles in protecting public rights); Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. Rev. 543 (2000) (commending the private enforcement of public rights).

161. 42 U.S.C. § 1974.

162. DOJ's monitoring powers under the Voting Rights Act are described in 42 U.S.C. § 1973f(d)(2) as extending to the power to "enter and attend at any place for tabulating the votes cast at any election held in such subdivision for the purpose of observing whether votes cast by persons entitled to vote are being properly tabulated." When software is used for tabulation, the unaided human eye is insufficient to ascertain whether the machine is counting accurately. Thus, DOJ must develop an understanding of what methods are available that will allow it to monitor whether "votes cast . . . are being properly tabulated."

As only one example of the need, electronic records of the vote tallies are not consistently maintained in South Carolina with its questionable elections in 2010 (see the first two sections of this chapter). Addressing the accountability lapse in the 2010 federal general election, Frank Heindel commented: "We continue to see problems across SC counties regarding the inability to properly store and reproduce the electronic files that are required to be kept for 22 months. . . . An audit of electronic voting records by South Carolina election officials did not include local files. . . ." Frank Heindel, *Orangeburg County Fails to Keep Electronic Election Files*, http://www.scvotinginfo.com/wp/2011/08/16/orangeburg-county-fails-to-keep-electronic-election-files/ (posted Aug. 16, 2011). Heindel also noted that the "State Election Commission has admitted that Lancaster County failed to keep any of their November 2010 election files for an audit." Frank Heindel, *Lancaster County Failed to Record Any Electronic Election Files*, http://www.scvotinginfo.com/wp/2011/08/16/lancaster-county-failed-to-record-any-electronic-election-files/ (posted Aug. 16, 2011).

Abundant evidence of nationwide failure to maintain appropriate electronic records of election activities conducted with e-voting systems has been developed, but DOJ has thus far not clarified the recordkeeping duties under § 1974.

163. DOJ's avoidance of voting systems legal issues may derive from Voting Section legal staff's lacking expertise in computer science and engineering, information systems security, and scientific knowledge of deployed e-voting systems. Correction of these staffing and information gaps will likely be necessary in order for DOJ to fulfill its HAVA-specified voting systems enforcement duties. While only a few election lawyers have developed technical voting systems expertise sufficient to support DOJ's legal monitoring and enforcement duties, talented scientists are available who are known for skillfully translating the technical and security points into concepts and points relevant for legal audiences.

To swiftly repair the information gap, DOJ could develop consultant and adviser relationships with technical experts independent of the vendors. For instance, the widely regarded scientists serving (or who previously served) on the EAC's Technical Guidelines Development Committee (TGDC) and the scientists who conducted the California TTBR and Ohio EVEREST studies of voting systems offer concrete knowledge of each deployed voting system's successes and deficiencies.

Computer scientists who have served on the NIST-EAC-sponsored TGDC include Doug Jones, David Wagner, and Ron Rivest; they also publish and speak on voting systems issues. Scientist Barbara Simons, a former ACM President and research scientist at IBM, possesses expertise in both voting systems and statewide voter registration databases; as an EAC Board of Advisers member, she is also knowledgeable about EAC policy positions that have not been technically well grounded. David Jefferson's national security insight has informed his voting systems work previously as the chair of California's Technical Advisory Board (on election technologies) and his work with the Department of Defense on Internet voting issues. All of these preeminent voting system experts possess significant expertise in post-election auditing methods, the primary check available on whether the voting system has counted accurately.

Supplying science and engineering expertise in assistive technologies, including for alternative (non-English) language needs, scientist and computer engineer Noel Runyan is singular in having amassed over 30 years in developing and testing assistive technologies of all types. Runyan's usability engineering expertise allows him to structure appropriate test contexts for determining whether a particular voting system's accessibility is merely asserted or fully realized, and for which types of disabilities. *See* NOEL H. RUNYAN, IMPROVING ACCESS TO VOTING: A REPORT ON THE TECHNOLOGY FOR ACCESSIBLE VOTING SYSTEMS (Voter Action and DĒMOS 2007); Noel Runyan & Jim Tobias, *Accessibility Review Report for California Top-to-Bottom Voting Systems Review*, http://www.sos.ca.gov/voting-systems/oversight/ttbr/accessibility-review-report-california-ttb-absolute-final-version16.pdf. Among Runyan's principles: "We must debunk the myth that we have to choose between accessible voting and verifiable voting. Democracy requires that we have both" (quoting Director Stanley J. Eichner of the Disability Law Center, Massachusetts) and those stated in *Americans with Disabilities Call for Election Systems Featuring Both Accessibility and Security, available at* http://www.voteraction.org/resources (Mar. 19, 2007).

All of these scientists have patiently and effectively educated many policymakers and lawyers (including this author).

164. For instance, until recently some states sought to protect against fraud by requiring notarization or witnessing of the voter's signature on the required paperwork. For some overseas voters, these requirements posed an insurmountable barrier. State calendars for completing their administrative tasks generally did not include sufficient time for blank ballots to be mailed overseas and returned by mail within the specified period for counting the ballot. Recent federal legislation has barred some of these practices for overseas and military voters.

165. Detailed in Pew Charitable Trusts, *No Time to Vote: Challenges Facing America's Overseas Military Voters* (Jan. 2009), Pew Center on the States, *available at* http://www.pewcenteronthestates.org/uploadedFiles/NTTV_Report_Web.pdf [hereinafter *Pew Study*].

166. *Id.*

167. Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), 42 U.S.C. §§ 1973ff–1973ff-7, *as amended by* Military and Overseas Voter Empowerment Act (MOVE), Pub. L. No. 111-84, subtitle H, §§ 575–589, 123 Stat. 2190, 2318–35 (2009) (MOVE Act).

168. Exec. Order No. 12,642, *Designation of the Secretary of Defense as the Presidential Designee Under Title I of the Uniformed and Overseas Citizens Absentee Voting Act* (June 8, 1988).

169. Remarks of FVAP Director Bob Carey, FVAP-NIST-EAC Workshop on UOCAVA Voting Systems, Washington, D.C. (Aug. 2010), *slides posted at* http://www.nist.gov/itl/csd/ct/uocava-2010-workshop-agenda.cfm.

170. For purposes here, "Internet voting" encompasses the marking and transmission of voted ballots over the public Internet. Online ballot-marking devices as well as complete systems that include the transmission of voted ballots to the election office for tabulation constitute "Internet voting."

171. *See infra* note 239.

172. 42 U.S.C. §§ 1973ff–1973ff-7 (2002).

173. *Id.* § 15301 *et seq.*

174. The Defense Department agency charged with UOCAVA voter assistance, FVAP, has urged states to permit all-electronic, Internet-based elections, despite the convergence of opinion by NIST and the security community that it is not technically possible to provide secure elections over the public Internet. These points and the discussion of the controversy that has ensued are developed more fully in text *infra* at *Federal Promotion of Problematic Internet Voting*, beginning after note 163.

175. This provision was revised in the 2004 NDAA and has arguably been superseded by the MOVE Act. *See infra* text accompanying notes 240–255.

176. The Overseas Vote Foundation and the Pew Charitable Trusts conducted studies that influenced the MOVE Act's structure and provisions. *See, e.g.*, Claire D. Smith, *It's in the*

Mail: Surveying UOCAVA Voters and Barriers to Overseas Voting (Overseas Vote Foundation Sept. 2009); *Pew Study, supra* note 165. More recently the Military Voters Protection Project has issued studies focused exclusively on military personnel and their families. *See* Eric Eversole, *Military Voting in 2010: A Step Forward, But a Long Way to Go, available at* http://mvp project.org/wp-content/uploads/2012/MVPProject_study_download.pdf.

177. MOVE Act, *amending* UOCAVA, *supra* note 167. To redress narrow issues, UOCAVA was amended several times before enactment of the omnibus MOVE Act, but these changes are not material to the analysis here.

178. *See Pew Study, supra* note 165.

179. 42 U.S.C. § 1973ff-1, *as amended by* the MOVE Act (2009).

180. Given that voting is a fundamental federal constitutional right, *see, e.g.*, Reynolds v. Sims, 377 U.S. 533, 561 (1964), and that right entails a vote that is counted and tallied as cast, *see supra* note 151, whether a jurisdiction is deploying a voting technology that functions adequately to assure that ballots are recorded, counted, and tallied as cast falls within the scope of federal constitutional voting rights concerns. Otherwise, the franchise right is theoretical but not actual and enforceable. As yet unresolved legal questions include whether Internet voting under present circumstances presents such significant opportunities for fraudulent tampering, blocking, or interception that it cannot suffice constitutionally as a voting method, and whether voting systems that provide only circular methods of verifying whether machine counts are accurate can reach the constitutionally minimum level of performance. The German Constitutional Court, for instance, declined to approve conducting national legislative elections on software-based voting systems that could not provide proof of the vote in ways an average person can understand without expert training. *See* Hoke, *supra* note 10, at note 157 (discussing Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 3, 2009, BVerfGE 123, 39–88, *available at* http://www.bverfg.de/entscheidungen/rs20090303_2bvc000307en.html, an opinion that invalidated the e-voting equipment used in Bundestag elections and held that public transparency in vote-counting processes is constitutionally required). The court's press office released an English summary of the decision, *see* Press Release no. 19/2009, Use of Voting Computers in 2005 Bundestag Election Unconstitutional (Mar. 3, 2009), *available at* http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019en.html (last visited May 14, 2012).

181. *See* the appendix, providing a chart showing state laws on ballot secrecy UOCAVA voters versus domestic voters. Verified Voting provides a U.S. map that graphically reflects which states permit specific types of voted ballot transmissions over the Internet. http://www.verifiedvotingfoundation.org/article.php?list=type&type=27.

182. *See id.* at text accompanying note 182 and appendix (ballot secrecy laws changing after FVAP lobbying). The ABA House of Delegates has recommended several steps to improve security and functionality of these new technological systems. *See* Resolution 114 (adopted unanimously, Aug. 9–10, 2010) (recommending studies and improved state and local defense in depth security practices for statewide voter registration databases), http://www.americanbar.org/content/dam/aba/directories/policy/2010_am_114.authcheckdam.pdf, and Resolution 121 (Aug. 8–9, 2011) (urging administrative steps for improved soundness of voter registration systems).

183. The Cuyahoga Election Review Panel observed that the federal primary is the most administratively complex of all the elections it must conduct. Ron Adrine, Tom Hayes & Candice Hoke, Cuyahoga Election Review Panel Final Report 5 (2006), http://urban.csuohio.edu/cei/public_monitor/CERP_Final_Report_20060720.pdf.

184. HAVA mandated the deployment of new federally funded voting technologies no later than the first federal election in 2006, according more than three years for technical development, marketing, and procurement, which was still substantially too little time for a radical shift in technologies. *See supra* text accompanying notes 84–86; *see also Voting and Registration Technology Issues*, *supra* note 9.

185. *I.e.*, UOCAVA, HAVA, and MOVE Act.

186. Techniques can include the use of DDOS (distributed denial of service attacks) and botnets.

187. Mobile phones commonly include monitoring software that reports on user conduct. This software could be "upgraded" to include reporting back to the vendor or service provider information about voting choices. For some examples of monitoring and unpermitted spying and data collecting in mobile phones, *see* Brad Spirrison, *iPhone Apps Storing Contact Lists Just the Latest Privacy Debacle in the Mobile Industry* (Feb. 16, 2012), http://www.appolicious.com/tech/articles/11090-iphone-apps-storing-contact-lists-just-the-latest-privacy-debacle-in-the-mobile-industry.

188. *See, e.g.*, Mark Baard, *NSF Preps New, Improved Internet*, Wired (Aug. 28, 2005) (reviewing GENI, the National Science Foundation's "major initiative that could lead to a completely new internet architecture, with built-in security measures and support for ubiquitous sensors and wireless communications devices"), http://www.wired.com/science/discoveries/news/2005/08/68667; *see also About GENI*, http://www.geni.net/?page_id=2.

189. "Mission critical" describes equipment and procedures that are essential to the successful functioning of the core operations of an organization. If a mission-critical piece of equipment fails, the business operations will fail.

190. Computer and network security constitute a subdivision of the information security field. Its objectives are defensive as well as facilitative—i.e., fostering users' ability to access and produce the information as desired. Computer and network security experts are trained in methods of protecting information from electronic theft, from unauthorized electronic modification, from "corruption" (errors that will affect transmission, retrieval, or processing, or that subject the original data to changes), and from natural disasters. Their focus includes the technical equipment or hardware, the software on which the information is created and managed, and security policies and practices. Expertise in computer security assists in protecting the information from software bugs, from external and remote threats over networks that include malware (e.g., viruses, worms, and botnets), and from "insiders" who might have become disloyal to the organization. *See generally* Matt Bishop, Computer Security: Art & Science (2002).

191. *See, e.g.*, Colorado legislative hearing, FVAP's representative Paddy McGuire (Feb. 2011) (recording in author's possession); *DoD Awards Grants for State & Local Military/Overseas Voting Systems* (Mar. 7, 2012) (announcing EASE grant funding awards), http://www.fvap.gov/resources/media/nr8-2012.pdf.

192. *See generally* David Jefferson & Candice Hoke, *The Dangers of Online and Onscreen Ballot Marking* (2012) (draft on file with author).

193. This author flagged the ambiguity and its damaging impact for FVAP's Director and its staff, but two years later the equivocation and failure to prominently and consistently warn of security dangers for voted ballots continue.

194. While election officials and policymakers are not conversant with or expert in network and computer security, they have had successful experiences personally and professionally with computer and Internet-based commercial sales and services. They will not necessarily recognize and will probably dispute the magnitude and gravity of these Internet-based election risks. Even when officials identify some of the new risks, particularly those posed by exposure of their election servers to the Internet, they may lack the budgets, technical expertise, and security infrastructural support that are essential for ensuring electoral integrity.

195. In a telephone interview with the author, FVAP's Principal Deputy Director Scott Wiedmann stated that it was not FVAP's responsibility to be concerned with the negative impact on a state's domestic voters or its election system as a whole. He said the agency's position is that UOCAVA and the MOVE Act charge FVAP only with improving *voting participation rates of UOCAVA voters* alone (Oct. 7, 2010).

196. Several factors reduce the likelihood of states' creating and maintaining the security infrastructures needed for MOVE Act and FVAP pilots that include returning voted ballots over the Internet. These factors include:

- Significant state and local budgetary deficits and reductions in personnel, with few exceptions throughout most of the nation;
- A diversity of local electoral administrative structures, personnel, and funding sources, some of which are much less well resourced than others;
- Smaller jurisdictions' increased use of outsourced technical support, without the capability of internal technical quality control and assurance;
- Lack of cyber security knowledge in the American population as a whole (presumably including election officials as well), as documented in other federal reports;
- The lack of technical and security expertise within much of the local election official (LEO) community and sometimes in the Secretary of State staffing;
- The rapid timetables for implementation of the MOVE Act and HAVA, leading to incomplete security infrastructure and network testing; and
- Numerous federal agencies' and departments' continued failure to meet information security standards, as documented by the GAO.

Given these factors and the complex security issues that Internet transmission of blank ballots presents, it is crucial that federal and state policymakers not simply assume that the essentials are present and then hold election officials accountable for conditions beyond their capacity. *See* Candice Hoke & Matt Bishop, *Essential Research Needed to Support UOCAVA-MOVE Act Implementation at the State and Local Levels,* one version published in the NIST-FVAP-EAC Workshop on UOCAVA Remote Voting Systems, http://www.nist.gov/itl/csd/ct/uocava_workshop_aug2010.cfm; updated version posted on the Social Science Research Network at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1697848 (citations omitted).

197. *See, e.g.*, FVAP/DoD, *Expanding the Use of Electronic Voting Technology for UOCAVA Citizens* (2007), http://www.fvap.gov/resources/media/ivas2007.pdf; FVAP/DoD, *Voting Over the Internet Pilot Project Assessment Report* (June 2001), http://www.fvap.gov/resources/media/voi.pdf.

198. For instance, the 2010 legislative initiatives document states, "FVAP recommends the expanded use of *email and online transmission for all election materials throughout the entire absentee voting process*, thereby supplementing fax and postal mail where possible" (emphasis added). http://www.fvap.gov/reference/laws/state-initiatives.html (last visited Sept. 12, 2011). The May 2011 FVAP plan for implementing the MOVE Act repeats this commitment: "FVAP also proposes the expanded use of email and online transmission for all election materials throughout the entire UOCAVA absentee voting process, replacing fax and postal mail where possible." Report on the Status and Implementation of Military and Overseas Voter Empowerment Act Programs, *transmitted by* the Under Secretary of Defense for Personnel and Readiness, at 19 (Mar. 2011), http://www.fvap.gov/reference/reports.html.

199. One example is Democracy Live's (DemLive's) technology, which FVAP is funding for deployment in multiple locations. In November 2011, DemLive marketing representatives confided to local election officials that their goal is to place "Internet voting in all the states." DemLive revealed their strategy: "[We] have to sneak up on it, step-by-incremental-step, to bring the public on board. . . . [We have all these Internet voting-ready] features that can be turned on one-by-one. First UOCAVA, then disabled voters, then all absentee voters, then eventually everyone else will be clamoring for what the others already have." [Anonymous election official], Notes of DemLive marketing presentation, November 2011 (on file with author).

200. The "digital divide" data suggest that access to the Internet is skewed in favor of the more affluent and Caucasian rather than being equally available to all demographic subsets. *See generally* Lee Rainie, Internet, Broadband, and Cell Phone Statistics (Jan. 2010), http://www.pewInternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics/Report.aspx.

201. *See* http://www.americanidolphonenumber.com/#.

202. *See* Joseph Lorenzo Hall, *Internet Voting in Union Elections*, https://freedom-to-tinker.com/blog/joehall/internet-voting-union-elections, explaining the ACCURATE research center's response to the U.S. Department of Labor's request for public comment on using the Internet for union elections:

> ACCURATE submitted a comment, http://accurate-voting.org/docs/comments/accurate-olms-comment-mar2011.pdf. The essential points we make are pretty straightforward: 1) don't allow internet voting from unsupervised, uncontrolled computing devices for any election that requires high integrity; and, 2) only elections that use voter-verified paper records (VVPRs) subject to an audit process that uses those records to audit the reported election outcome can avoid the various types of threats that DOL is concerned with. The idea is simple: VVPRs are independent of the software and hardware of the voting system, so it doesn't matter how bad those aspects are as long as there is a robust parallel process that can check the result. Of course, VVPRs are no panacea: they must be carefully stored, secured and transported and ACCURATE's HCI researchers have shown

that it's very hard to get voters to consistently check them for accuracy. However, those problems are much more tractable than, say, removing all the malware and spyware from hundreds of thousands of voter PCs and mobile devices.

203. Some credit unions also use telephonic voting methods. *See* CUBallot.com, https://www.cuballot.com/telephonevoting.html.

204. *See, e.g.*, the Constitution's Preamble and the Guarantee Clause, U.S. Const. art. IV, § 4.

205. The Court's citations include Ex parte Siebold, 100 U.S. 371 (1877); United States v. Mosley, 238 U.S. 383, 386 (1915); United States v. Saylor, 322 U.S. 385 (1944); Baker v. Carr, 369 U.S. 186 (1962); Gray v. Sanders, 372 U.S. 368, 380 (1963); and Reynolds v. Sims, 377 U.S. 533, 554–55 (1964).

206. HAVA has codified an exceptionally low error rate for voting systems used in federal elections that would include Internet systems. 42 U.S.C. § 15481(a)(5). It incorporates by reference the FEC's 2002 standard. In Broken Ballots, *supra* note 1, at 135–41, the authors critique this standard. Arguably, a voting system's "error rate" reflects malfunctions of all kinds, from all causes, including system failure to accurately record the voter's choices, and failure to accurately tabulate and report race results, whether caused by hardware fault, software bug, or configuration error, and many other sources.

207. This list of legally mandated voting system properties is not exhaustive but focuses on four central, widely required capabilities. The federal Voluntary Voting System Guidelines provide content to these four and other recommended properties or attributes. *See* http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx.

208. David Jefferson, correspondence with author, May 20, 2012. Jefferson stressed that while both web portal and e-mailed voted ballots lack privacy protections, e-mailed ballots are considerably worse. While encrypted web portal ballots are vulnerable to spying primarily at the outset and recipient election office locations rather than at every transmission point, e-mailed ballots offer a multitude of opportunities for spying, data collection of voters' choices, and possibly tampering with those choices. "E-mail voting is decrypted and re-encrypted at each forwarding hop and at the final server at the receiver's ISP. Privacy can be violated at several points along the way between the voter and election office. . . . With web portal voting, privacy can only be violated at the end points of the communication." *Id.*; *see also* David Jefferson, *If I Can Shop and Bank Online, Why Can't I Vote Online?*, http://verifiedvoting.org/downloads/votingtransactions/ (last visited Feb. 12, 2012); Candice Hoke, *Internet Voting: Structural Governance Principles for Election Cyber Security in Democratic Nations*, Internet Voting: Formulating Structural Governance Principles for Elections Cybersecurity, proceedings of ISGIG 2009: Second International Symposium on Global Information Governance, September 15–17, 2009, Prague, Czech Republic; published in ACM Library, http://dl.acm.org/citation.cfm?id=1920329.

209. David Jefferson, correspondence with author, May 20, 2012.

210. Professor Alex Halderman led his graduate students in attacking the District of Columbia's Internet voting system, planned for launch with real votes in the November 2010 general election barely three weeks hence. To their credit the D.C. Board of Elections and

Ethics planned a public test. The team's remote attack resulted in their substitution of science fiction write-in candidates on 100% of the ballots. Media coverage includes: slashdot, *In Theory and Practice, Why Internet-Based Voting Is a Bad Idea* (Mar. 2, 2012) (hereinafter *Bad Idea*), http://politics.slashdot.org/story/12/03/02/1940236/in-theory-and-practice-why-internet-based-voting-is-a-bad-idea; Jaikumar Vijayan, *Internet Voting Systems Too Insecure, Researcher Warns* (Mar. 1, 2012), http://www.computerworld.com/s/article/9224799/Internet_voting_systems_too_insecure_researcher_warns?taxonomyId=17&pageNumber=2; Alex Altman, *Will Online Voting Turn Into an Election Day Debacle?*, TIME, Oct. 15, 2010, http://www.time.com/time/printout/0,8816,2025696,00.html; *see also* Editorial: *Flaws in D.C.'s Online Voting System Should Serve As a Warning to All States* (Oct. 18, 2010), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/10/18/AR2010101804529.html (last visited April 30, 2012). The team's academic article discussing their attack can be found at Scott Wolchak, et al., *Attacking the Washington, D.C. Internet Voting System*, Proc. 16th Conference on Financial Cryptography & Data Security (Feb. 2012), https://jhalderm.com/pub/papers/dcvoting-fc12.pdf. Halderman says the exercise was meant to educate election officials about the dangers of online voting. "The question is not whether these systems can be broken into," he says. "It's whether anyone wants to." *See* Altman, *supra*. For a discussion of issues directed to the legal audience, *see* Jeremy Epstein, *Internet Voting, Security, Privacy*, 19 WM. & MARY BILL RTS J. 885 (2011) (explaining the technical problems and their dangerous impact for voting rights and election integrity).

211. These attacks have sought to achieve intellectual property theft, industrial espionage, vandalism, and governmental embarrassment, among other objectives.

212. Ronald L. Rivest, Thoughts on UOCAVA Voting, Presentation at Workshop on UOCAVA Remote Voting Systems (Aug. 6, 2010), *slides available at* http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/RIVEST_2010-08-05-uocava.pdf. As David Jefferson has noted, "Even if a jurisdiction has appropriate security expertise and vigilant network supervision, it is still at risk for all [the dangerous] consequences. [Computer science does] not know how to eliminate these risks. . . . [A] jurisdiction that exposes its voting infrastructure to the Internet has essentially no chance of successfully defending against a competent determined attack." Jefferson, message to author, Oct. 17, 2010 (on file with the author).

213. David Jefferson, *If I Can Shop and Bank Online, Why Can't I Vote Online?*, http://electionlawblog.org/wp-content/uploads/jefferson-onlinevoting.pdf (last visited May 12, 2012).

214. "The Zeus malware has been a significant issue for banks. It is capable of intercepting login credentials in real-time on an infected computer and carrying out immediate transactions. Zeus is also frequently undetected by antivirus software." Jeremy Kirk, *Researchers See Updated Zeus Malware*, http://www.computerworld.com/s/article/9219489/Researchers_see_updated_Zeus_malware?source=CTWNLE_nlt_security_2011-08-25&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+computerworld%2Fs%2Ffeed%2Ftopic%2F85+%28Computerworld+Malware+and+Vulnerabilities+News%29. "After sneaking onto a PC via an exploit, the Zeus bot watches for, then silently captures log-in credentials for a large number of online banks, as well as usernames and passwords for Schwab accounts. The attack code also injects a bogus form that asks victims to provide additional information the

thieves can later use to confirm that *they* are the legitimate owner of the Schwab investment account. On that form are fields asking for the user's mother's maiden name, driver license number and employer." Gregg Keizer, *Zeus Botnet Gang Targets Charles Schwab Accounts; Attacks Vulnerable PCs to Steal Full Access to Investments, Cash* (Oct. 16, 2010), http://www.computerworld.com/s/article/9191479/Zeus_botnet_gang_targets_Charles_Schwab_accounts.

215. As has been set forth by several preeminent academic cyber security experts (MIT's Ron Rivest and UC Berkeley's David Wagner), NIST scientists, and the SERVE Report scientists (2004), returning voted ballots over the insecure public Internet severely jeopardizes the security of our nation. They all have identified the transmission of voted ballots over the public Internet as presenting an unusually attractive and achievable target for numerous adversaries, foreign and domestic. The slides from these scientists' talks delivered at the NIST-EAC-FVAP workshop on UOCAVA Solutions present their risk assessments and recommendations to avoid Internet voting. *See* http://www.nist.gov/itl/csd/ct/uocava-2010-workshop-agenda.cfm (Aug. 2010). *See also* NISTIR, *A Threat Analysis of UOCAVA Voting Systems*; NISTIR 7682, *Information System Security Best Practices for UOCAVA-Supporting Systems* (Apr. 2010); NISTIR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*.

216. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011): "A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access."

217. As computer security expert Bruce Schneier has commented:

> Different [encryption] algorithms offer different degrees of security; it depends on how hard they are to break. If the cost required to break algorithms is greater than the value of the encrypted data, then you're probably safe. If the time required to break an algorithm is longer than the time the encrypted data must remain secret, then you're probably safe. If the amount of data encrypted with a single key is less than the amount of data necessary to break the algorithm, then you're probably safe.
>
> I say "probably", because there is always a chance of new breakthroughs in cryptanalysis.

BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 8 (2d ed. 1996).

218. Computer scientists and voting system specialists Barbara Simons and Doug Jones have written:

> Some systems, such as Helios and Remotegrity provide cryptographic tools to allow the voter to verify that an accurate version of her ballot has been received and counted. Encryption does not protect against Denial of Service attacks, spoofing, coercion, design flaws, and many kinds of ordinary software bugs. If a serious problem is uncovered in an election, there is no way to conduct a recount. While these systems have been used for some small elections, the general consensus is that they are not ready for use in a major election.

They quote cryptographer Ben Adida, the creator of Helios, who underscored the security limitations of electronic voting:

> We now have documented evidence . . . that viruses like Stuxnet that corrupt nuclear power plants by spreading from one Windows machine to the other have been built. And so if you run a very large scale election for a president of a G8 country, why wouldn't we see a similar scenario? Certainly, it's worth just as much money; it's worth just as much strategically. . . . All the verifiability doesn't change the fact that a client side corruption in my browser can flip my vote even before it's encrypted, and if we . . . must have a lot of voters verify their process, I think we're going to lose, because most voters don't quite do that yet.

Broken Ballots, *supra* note 1, at 278–79 (citations omitted). Nonetheless, Internet voting vendors continue to claim their products achieve security and privacy. *See, e.g.*, Scytl Press Release, Scytl Unveils Secure Online Voting on Google Android and Apple iOS Devices, *available at* http://www.marketwatch.com/story/scytl-unveils-secure-online-voting-on-google-android-and-apple-ios-devices-2012-05-14.

219. Encryption, or cryptosystems, over time are subject to mathematical discoveries that can permit their penetration. For instance, the U.S. Data Encryption Standard (DES) was officially adopted in 1976. A message encrypted using DES was first broken in public in 1997. *See* https://en.wikipedia.org/wiki/Data_Encryption_Standard. DES was finally withdrawn as an encryption standard for government use in 2005. *See* Notices, 70 Fed. Reg. 28,907 (May 19, 2005), *available at* http://csrc.nist.gov/publications/fips/05-9945-DES-Withdrawl.pdf.

220. For instance, a May 2009 Hawai'i Internet election for a neighborhood race produced sharply lower turnout rates than the prior election, but no independent investigation was undertaken to determine whether voted ballots had not been delivered. The vendor simply pronounced it a "historic success," and the jurisdiction saved money over conventional elections. A town official commented that voters did not "bother" to vote, without understanding that voters may have cast ballots that were not received and counted. *Voting Drops 83 Percent in All-Digital Election; People Could Vote Online, on Phone for Neighborhood Board*, http://www.kitv.com/politics/19573770/detail.html#ixzz1YLb4NcnQ. The vendor whom the town paid to conduct the election produced an effusive press announcement claiming that the election was a "historic success." *See Historic Success to Be Repeated with All-Digital Election by Everyone Counts; Honolulu Again Chooses Everyone Counts to Provide Universal Access Elections*, http://www.everyonecounts.com/news/press-releases/72-historic-success-to-be-repeated-with-all-digital-election-by-everyone-counts ("The City and County of Honolulu have selected Everyone Counts, Inc.—a world leader in transparent, secure, and accessible elections for all voters—to deliver Internet and telephone voting for the 2011 Neighborhood Board Elections. This year's election will build upon 2009's success and historical landmark, as it became the nation's first all-digital election.").

221. 42 U.S.C. §§ 1973ff-1(a)(6)–(7).

222. Professor Ron Rivest has stated:

> At some point in the far distant future—perhaps by mid-century—the see-saw battle between attack and defense for computer and internet security will have settled down with a total victory for the defenders. But I'm not particularly optimistic about this. If that should happen, then perhaps we'll have some sort of voting method where you can vote in an auditable and uncoercable manner . . . with communications secured by unbreakable cryptography, in a manner where your vote is necessarily private and visible only to you. [But such a vision] would require decades of progress on many fronts to realize.

Remarks on the Future of Election Integrity, MIT: Election Integrity: Past, Present, and Future workshop (Oct. 1, 2011).

223. The MOVE Act specified remedial activities by the Military Postal Service Agency (MPSA), including a requirement to postmark the absentee ballot on the day it is collected and to provide expedited mail delivery. The MPSA Report to Congress on the 2010 service to UOCAVA voters revealed that the MPSA is able to deliver voted ballots from the troops back to county election headquarters averaging only 5.2 days, with "92% of absentee ballots reach[ing] election offices within 7 days." FVAP has posted the report at http://www.fvap.gov/resources/media/2010_MPSA_after_action_report.pdf.

224. *See* http://www.overseasvote.org.

225. Former FVAP Deputy Director Scott Wiedmann reported that DoD is updating and revising the Directives governing FVAP activities as this chapter goes to press. Others have argued the FVAP has historically neglected its voter registration duties under the National Voter Registration Act, 42 U.S.C. § 1973gg-1 *et seq. See* Military Voter Protection Project, *Military Voting in 2010.* The Project's Executive Director, Eric Eversole, also recommends that FVAP focus on augmenting military service members' absentee ballot requests, noting that only 15.8 percent of military voters requested an absentee ballot in 2010.

226. *See* appendix (chart of ballot-secrecy laws).

227. National Defense Authorization Act of 2002, Pub. L. No. 107-107, 115 Stat. 1277 (2001).

228. Secure Electronic Registration and Voting Experiment (SERVE). *See* http://www.servesecurityreport.org.

229. *See* http://servesecurityreport.org/.

230. *Id.* Executive Summary conclusion h.

231. Directive 1000.04 provides in pertinent part:

> 4.3. Every eligible voter shall:
>
> 4.3.1. Be given, unless military necessity precludes it, an opportunity to register and vote in any election for which he or she is eligible.
>
> 4.3.2. Be able to vote in person or by absentee process when local conditions allow the voter to participate in the electoral process.
>
> 4.3.3. *Receive voting assistance in a manner that safeguards the integrity of the electoral process* and *secrecy of the ballot*.
>
> 4.4. *All persons assisting in the voting process shall take all necessary steps to prevent fraud and to protect voters against any coercion . . . .*

(Emphasis added.) *Available at* http://www.dtic.mil/whs/directives/corres/pdf/100004p.pdf (last visited April 30, 2012).

232. FVAP employees have confidentially acknowledged to this author that the FVAP is seeking changes in DoD Directive 1000.04 that would eliminate the requirement for DoD staff to protect ballot secrecy. Given that FVAP has been lobbying state governments for many years for no ballot secrecy requirement, despite its violation of Directive 1000.04, and has achieved this outcome for UOCAVA voters in over three-fifths of the states, the FVAP's formal request for the Directive's elimination is not surprising. FVAP's record manifests little understanding and respect for fundamental election law principles, such as ballot secrecy's role in protecting systemic electoral integrity.

233. Computer Technologists' Statement on Internet Voting (Sept. 11, 2008), http://www.voteraction.org/files/Computer%20Scientist%20Internet%20Voting%20Statement.pdf.

234. FVAP, Report on the Status and Implementation of Military and Overseas Voter Empowerment Act Programs, *transmitted by* the Under Secretary of Defense for Personnel and Readiness, at 19 (Mar. 2011), http://www.fvap.gov/reference/reports.html (emphasis added).

235. E.g., in FVAP's legislative initiatives on which it seeks state action, the 2010 version comments:

> Given that the MOVE Act requires States send ballots to voters at least 45 days before the election and to send them electronically as well as by postal mail, FVAP *recommends the expanded use of email and online transmission for all election materials throughout the entire absentee voting process*, thereby supplementing fax and postal mail where possible.

http://www.fvap.gov/reference/laws/state-initiatives.html (last visited Sept 12, 2011) (emphasis added). This policy statement recommends the permissibility of conducting all election tasks over the Internet as a "supplement" rather than as a "replacement" for postal and fax transmissions. This revision continues to violate Directive 1000.04. *See also* FVAP, *Voting Over the Internet Pilot Project Assessment Report* (June 2001), which often has a cheerleading tone but occasionally includes remarks about security and election integrity. For instance, at 10:

> [t]he *biggest question regarding the use of the Internet for registration and voting is whether the integrity of the electoral process can be preserved*. There are a number of elements to be considered relative to *whether this technology can provide sufficient security, secrecy, and transparency of the process to be relied upon for the exercise of this most fundamental of Constitutional rights*. Another major concern is the *potential for election fraud when using the Internet* [emphasis added].

236. See the appendix for an inventory of state ballot-secrecy laws.

237. *See, e.g.*, presentations by Professors Ron Rivest, David Wagner, and David Jefferson at the FVAP-NIST-EAC Workshop on UOCAVA Voting Systems, Washington, D.C. (Aug. 2010), *slides posted at* http://www.nist.gov/itl/csd/ct/uocava-2010-workshop-agenda.cfm.

238. FVAP Grants webpage with link to solicitation, http://www.fvap.gov/leo/grants.html.

239. When compared to other parts of the DoD budget, $20 million may not seem mammoth. But these FVAP monies are virtually the only governmental source of research and development funds currently and prospectively available for developing new election technologies. As such, the grant program exerts a colossal impact on setting the future technical direction and capabilities for voting. As currently structured, the grant program constitutes a worrisome, apparently DoD-approved inducement of state and local governments into highly insecure methods of voting when other more secure (and cheaper) methods are available that better protect both the voter's participation interests and systemic electoral legitimacy.

240. President Obama has promulgated a strict ethics policy designed to prevent "revolving door" regulators. The FVAP Deputy Director for Technology may fall within these bans. *See* Exec. Order No. 13,490 (Jan. 21, 2009):

> 2. *Revolving Door Ban—All Appointees Entering Government*. I will not for a period of 2 years from the date of my appointment participate in any particular matter involving specific parties that is directly and substantially related to my former employer or former clients, including regulations and contracts.
>
> 3. *Revolving Door Ban—Lobbyists Entering Government*. If I was a registered lobbyist within the 2 years before the date of my appointment, in addition to abiding by the limitations of paragraph 2, I will not for a period of 2 years after the date of my appointment:
>
> (a) participate in any particular matter on which I lobbied within the 2 years before the date of my appointment;
>
> (b) participate in the specific issue area in which that particular matter falls . . . .

241. National Defense Authorization Acts: H.R. 4200, Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Oct. 8, 2004), 150 Cong. Rec. H 9187 (2004); National Defense Authorization Act for Fiscal Year 2005, Committee on Armed Services, H.R. Rep. No. 491, 108th Cong. (2004); Section 592 Repeal of Requirement to Conduct Electronic Voting Demonstration Project for the Federal Election to Be Held in November 2004, National Defense Authorization Act for Fiscal Year 2002, Section 552, Committee on Armed Services, H.R. Rep. No. 194, 107th Cong. (2001).

242. Notably, Congress did not specify that this "electronic voting system" must utilize the Internet. Nor did it specify that every aspect of the system be electronic, as FVAP Director Carey has sometimes represented. National Defense Authorization Act of 2002, § 1604, Pub. L. No. 107-107, 115 Stat. 1012, 1277 (2002), reads in pertinent part:

> § 1604. Electronic Voting Demonstration Project.
>
> (a) Establishment of Demonstration Project.—
>
> (1) In General.—Subject to paragraph (2), the Secretary of Defense shall carry out a demonstration project under which absent uniformed services voters are *permitted to cast ballots in the regularly scheduled general election for Federal office for November 2002* through an *electronic voting system*. The project shall be carried out with participation of suf-

> ficient numbers of absent uniformed services voters so that the results are statistically relevant.
>
> (2) Authority to Delay Implementation.—If the Secretary of Defense determines that the implementation of the demonstration project under paragraph (1) with respect to the regularly scheduled general election for Federal office for November 2002 *may adversely affect the national security of the United States*, the Secretary *may delay* the implementation of such demonstration project until the regularly scheduled general election for Federal office for November 2004. The Secretary shall notify the Committee on Armed Services and the Committee on Rules and Administration of the Senate and the Committee on Armed Services and the Committee on House Administration of the House of Representatives of any decision to delay implementation of the demonstration project.
>
> (b) Coordination With State Election Officials.—The Secretary shall carry out the demonstration project under this section through cooperative agreements with State election officials of States that agree to participate in the project.
>
> (c) Report to Congress.—Not later than June 1 of the year following the year in which the demonstration project is conducted under this section, the Secretary of Defense shall submit to Congress a report analyzing the demonstration project. The Secretary shall include in the *report any recommendations* the Secretary considers appropriate for *continuing the project on an expanded basis for absent uniformed services voters during the next regularly scheduled general election for Federal office.*

(Emphasis added.)

243. The EAC's Report to Congress with its "roadmap" to Internet voting comments, "Four states participated in this experiment, which enabled voters to use their own personal computers to securely register to vote, request and receive [blank] absentee ballots, and return their voted ballots." *UOCAVA Pilot Program Testing Requirements, Uniformed and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements*, United States Election Assistance Commission (Mar. 24, 2010), *available at* http://www.eac.gov/assets/1/AssetManager/UOCAVA_Pilot_Program_Requirments-03.24.10.pdf.

244. *See* David Jefferson et al., *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, Servesecurityreport.org (Jan. 20, 2004), *available at* http://www.servesecurityreport.org/.

245. Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Pub. L. No. 108-375, § 567, 118 Stat. 1811, 1919 (2004).

246. Conference Rep. on H.R. 4200, Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Oct. 8, 2004), 150 Cong. Rec. H 9187 (2004), reads thus:

> The House bill . . . would repeal the requirement . . . for the Secretary of Defense to conduct a demonstration project to permit absentee uniformed service voters to cast their ballots through an electronic voting system. The

> Senate amendment . . . would authorize delay in carrying out an electronic voting demonstration project until November 2006. The House recedes with an amendment that would delay the electronic voting demonstration project . . . .
>
> The Department of Defense's Secure Electronic Registration and Voting Experiment (SERVE) was an important prototype for electronic voting that should not be abandoned.

247. Bob Carey, *UOCAVA 2010 Workshop Agenda, FVAP Views on Solutions & Challenges: NIST-EAC-FVAP Workshop on UOCAVA Voting Systems*, National Institute of Standards and Technology (Aug. 6, 2010), *available at* http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/CAREY_FVAP_Presentation_to_NIST-EAC-FVAP.pdf.

248. *See generally* Reed Dickerson, The Interpretation and Application of Statutes 138–60 (1975).

249. Robert Carey, Opening Address of FVAP Director, Workshop on UOCAVA Remote Voting Systems (Aug. 6, 2010), http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/CAREY_FVAP_Presentation_to_NIST-EAC-FVAP.pdf.

250. Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens, GAO-07-774, United States Government and Accountability Office [hereinafter GAO] (June 2007), *available at* http://gao.gov/assets/270/262023.pdf. The primary author of this report, Derek B. Stewart, previously held the title of Director of the Defense Capabilities and Management. He served as lead author of numerous GAO testimonies and studies of military personnel management issues. *See, e.g.*, Military Personnel: Preliminary Observations on Recruiting and Retention Issues Within the U.S. Armed Forces, GAO-05-419T, GAO (Mar. 2005), *available at* http://www.gao.gov/new.items/d05419t.pdf; DoD Personnel Clearances: Government Plan Addresses Some Long-standing Problems with DOD's Program, But Concerns Remain, GAO-06-233T (2005), http://www.fas.org/sgp/gao/gao-06-233t.pdf.

251. Rivest, *supra* note 222, at 2 (emphasis added).

252. These points are discussed in *supra* text accompanying notes 177–183.

253. *See* United States v. Fausto, 484 U.S. 439. 453 (1988), in which the Court notes, "Th[e] classic judicial task of reconciling many laws enacted over time, and getting them to 'make sense' in combination, necessarily assumes that the implications of a statute may be altered by the implications of a later statute." The Court also observed that construing a statute to incorporate an implied amendment is particularly appropriate when Congress has replaced ad hoc terms with an "integrated scheme." *Id.* at 445. These interpretive guides are equally apt for the MOVE Act's revision of a series of NDAA provisions over almost a decade while the nation was learning that the Internet presented egregious new attack and crime opportunities and not merely positive communication capabilities.

254. *See* 42 U.S.C. § 1973ff-2b, which provides:

> Nothing in this section shall relieve the Presidential designee of their duties and obligations under any directives or regulations issued by the Department

> of Defense, including the Department of Defense Directive 1000.04 (or any successor directive or regulation) . . . .

255. *See, e.g.*, PBS News Hour, *Internet Voting: Will Democracy or Hackers Win?* Feb. 16, 2012 (including segment with Director Carey discussing his efforts to fulfill the legislative "mandate" for an Internet boting pilot), http://www.pbs.org/newshour/bb/politics/jan-june12/internetvoting_02-16.html?print.

256. This author, among others, attempted to persuade Director Carey not to fund electronic voting system components merely on the basis of marketing representations and instead to require robust independent validation of their compliance with HAVA and constitutional requirements.

257. The difficulty and yet the need for improving UOCAVA voter registration rates was underscored in separate discussions in September 2011 with both Susan Dzieduszycka-Suinat, President, Overseas Vote Foundation, and Eric Eversole, Director of the Military Voter Protection Project. Confirming their views, see *OVF Research and Reports*, Overseas Vote Foundation, https://www.overseasvotefoundation.org/research-intro-OVF-reports (last visited Mar. 18, 2012); Eric Eversole, *Military Voting in 2010: A Step Forward, But a Long Way to Go*, Military Voter Protection Project (July 2011), *available at* http://mvpproject.org/in-the-news/mvp-project-report-highlites-military-voting-in-2010/.

258. Two resources outline robust quality assurance techniques for ensuring tabulation accuracy. *See Evidence-Based Elections*, *supra* note 21; Mark Lindeman and Philip B. Stark, *A Gentle Introduction to Risk-Limiting Audits*, IEEE Security and Privacy (forthcoming 2012), *draft available at* http://statistics.berkeley.edu/~stark/Preprints/gentle12.pdf (last visited Apr. 28, 2012).