Case Western Reserve Law Review

Volume 62 | Issue 4 Article 6

2012

Judicial Protection of Popular Sovereignty: Redressing Voting Technology

Candice Hoke

JUDICIAL PROTECTION OF POPULAR SOVEREIGNTY: REDRESSING VOTING TECHNOLOGY

Candice Hoke[†]

Over the past decade, Ohio, California, Florida, and other states commissioned over a dozen separate, independent scientific assessments of their deployed or contemplated electronic voting systems. Each published report documented grave deficiencies that relate to these systems' capacity to accurately record vote choices, produce correct tallies, and function reliably and securely in other ways that integrally relate to the right to vote.[1] The most

[†] Associate Professor of Law, Cleveland State University; Founding Director of the Center for Election Integrity and Project Director of the *Public Monitor of Cuyahoga Election Reform* (2006–08); Research Team Leader for a portion of the California *Top to Bottom Review of Voting Systems* (2007); and pro bono consultant for structuring the Ohio EVEREST voting system review. Under Public Monitor auspices, she authored or co-authored reports on election technical security, and proposed and led Ohio's first post-election audit of cast ballots. The author has testified before the U.S. House of Representatives, Committee on Administration, on post-election auditing and before the U.S. Election Assistance Commission on voting system "incidents reporting." In work to improve voting technologies, she works with election officials nationally, congressional and state legislative staff of both major political parties, and with executive office staff at federal and state levels. The author thanks Professors Richard Hasen and Dan Tokaji, who have dedicated part of their scholarly agendas to grappling with voting technology issues, and scientists Matt Bishop, David Jefferson, Barbara Simons, Andrew Appel, Ron Rivest, Doug Jones, Alex Halderman, Duncan Buell, Dave Eckhardt, Jeremy Epstein, and David Wagner, who persist in seeking resolutions to e-voting deficiencies. She also thanks scholars in allied fields, election officials, and advocates for election operations accountability who include Doug Kellner, Philip Stark, Mark Lindeman, Matt Damschroder, Robert Adams, Susannah Goodman, Pam Smith, Lowell Finley, Jane Platten, Howard Stanislevic, Ellen Theisen, Susan Greenhalgh, Luther Weeks, and Margit Johansson. Critical commentary was generously provided by Professors Richard Hasen, George H. Taylor, and James Wilson but errors are the author's alone. Superb research assistance from law student Sarah Kendrig and law librarians Amy Burchfield, Tom Hurray, and Schuyler Cook proved essential.

[1] *See* Matt Bishop, Mark Graff, Candice Hoke, David Jefferson & Sean Peisert, *Resolving the Unexpected in Elections: Election Officials' Options,* app. 2, 22–27 (2008), http://nob.cs.ucdavis.edu/bishop/notes/2008-forensic/2008-eforen.pdf (providing a comprehensive listing of the studies through 2008 and links to their public reports and a guide to

comprehensive and definitive of these studies, the California Top to Bottom Review and the Ohio Project EVEREST assessment, each evaluated three major voting systems in nationwide deployment.[2] Collectively, these two studies confirm prior studies' findings detailing significant deficiencies in the voting equipment used by over 90 percent of all American voters.[3]

While information security specialists and computer scientists have published numerous peer-reviewed articles and held conferences devoting significant attention to these two studies,[4] rather surprisingly no election law scholar has published a law review article that considers the legal import of these comprehensive findings from top scientists.[5] This stunning silence from the election law scholarly

indicators of possible electronic malfunctions and forensic assessments to determine whether the tabulation reports deserve trust).

[2] The Top to Bottom Review ("TTBR") evaluated Diebold, Sequoia, and Hart InterCivic branded voting systems and reports on the voting systems have been available on the Secretary of State's website since they were issued in August 2007. *Top-to-Bottom Review*, CALIFORNIA SECRETARY OF STATE DEBRA BOWEN, http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm (last visited April 15, 2012) [hereinafter TTBR]. EVEREST studied ES&S, Diebold, and Hart. *Systems and Internet Infrastructure Security*, *Ohio EVEREST Voting Study,* PENN STATE UNIV., http://siis.cse.psu.edu/everest.html (last visited May 10, 2012).

[3] The conservative estimate that these systems are used by 90 percent of all U.S. voters is generated from the U.S. Department of Justice's judicial submission of antitrust legal documents. These reveal that the merger of the former Diebold Election Systems division (renamed Premier Elections Solutions) with ES&S, Inc. would have concentrated control over 70 percent of the U.S. electorate in the hands of buyer ES&S. *See* Press Release, U.S. Dep't of Justice, Justice Department Requires Key Divestiture in Election Systems & Software/Premier Election Solutions Merger (March 8, 2010), *available at* http://www.justice.gov/opa/pr/2010/March/10-at-235.html (reporting ES&S' divestiture of voting equipment system assets purchased from Premier Elections Solutions in order to restore competition as part of a settlement agreement with the Department of Justice Antitrust Division). By adding jurisdictions using Sequoia and Hart InterCivic systems (the third- and fourth-largest companies), the voting systems of at least 90 percent of all voters, and more likely 95–98 percent, are embraced within these two studies. *See* TTBR, *supra* note 2 (detailing Secretary Bowen's decisions and the independent experts' findings in the review).

[4] The Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE) is the prominent international interdisciplinary scholarly forum dedicated to voting technology issues. It posts a call for papers every spring. Part of the USENIX Security conference proceedings, its papers are peer–reviewed and web–published without charge. Several 2008 conference papers present scholarly versions of the reports produced in the TTBR or EVEREST. *See, e.g.*, Adam Aviv et al., *Security Evaluation of ES&S Voting Machines and Election Management System* (2008), http://static.usenix.org/events/evt08/tech/full_papers/aviv/aviv.pdf; Kevin Butler et al., *Systemic Issues in the Hart InterCivic and Premier Voting Systems: Reflections on Project EVEREST* (2008), http://static.usenix.org/events/evt08/tech/full_papers/butler/butler.pdf. Papers published in later EVT/WOTE conferences continue to draw on these two studies. *E.g.,* D.A. Buell et al., *Auditing a DRE–Based Election in South Carolina* (2011), http://static.usenix.org/events/evtwote11/tech/final_files/Buell.pdf (relying on EVEREST's ES&S reports); Matt Bishop et al., *E-Voting and Forensics: Prying Open the Black Box* (2009), http://static.usenix.org/events/evtwote09/tech/full_papers/bishop.pdf.

[5] A Westlaw JLR database search identified a small number of articles citing to the

community sharply contrasts with the profuse legal scholarship that evaluated *Bush v. Gore*'s handling of punch card voting inadequacies and the Florida presidential debacle.[6] The scholarly muteness also differs markedly from the rapt attention accorded to campaign finance,[7] redistricting,[8] and voter registration *cum* voter fraud.[9]

TTBR and EVEREST, but none, however, has been authored by an election law scholar who assessed the import of these findings with regard to the constitutional standards for the right to vote. *See, e.g.,* Danielle Keats Citron, *Open Code Governance*, 2008 U. CHI. LEGAL F. 355, 358 (recommending open source software for mission–critical governmental activities including voting); Brian J. Miller, *The Right to Participate, the Right to Know, and Electronic Voting in Montana*, 69 MONT. L. REV. 371, 390 (2008) (concluding that Montana law proscribes the use of unauditable voting systems). Daniel Tokaji is one of the few election legal scholars who considered the legal import of early scientific voting system studies. *See generally* Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values,* 73 FORDHAM L. REV. 1711 (2005) [hereinafter *Electronic Voting and Democratic Values*] (providing an overview of the transformation of the voting process's recent emphasis on electronic voting and from both a legal and policy perspective). Tokaji has not yet reassessed his early approach in light of the much more comprehensive, definitive studies from California and Ohio, and in light of the experiential record amassed by these e-voting technologies. This Article seeks in part to garner Tokaji's revisiting of voting technology legal questions in light of the materials and arguments advanced here. Book treatments, however, address some of these issues. *E.g.,* RICHARD HASEN, THE VOTING WARS (2012) (including a chapter on voting technology disputes). Election Law casebooks, however, thus far exclude attention to these definitive studies and their import for election law values.

[6] *See, e.g.,* Edward B. Foley, *The Future of* Bush v. Gore?, 68 OHIO ST. L.J. 925, 1006 (2007)(exploring the continuing value and legal issues posed by the seminal case, including appropriate constitutional standards of review for election administration issues); Richard L. Hasen, *The Untimely Death of* Bush v. Gore, 60 STAN. L REV. 1 (2007) (lamenting the decision's import in election administration); Richard H. Pildes, *The Supreme Court, 2003 Term–Foreword: The Constitutionalization of Democratic Politics,* 118 HARV. L. REV. 29, 49 (2004); Louise Weinberg, *When Courts Decide Elections: The Constitutionality of* Bush v. Gore. 82 B.U. L. REV. 609 (2002) (reconsidering the constitutionality of Supreme Court intruding into a presidential election as occurred in 2000). Rick Hasen helpfully inventoried *Bush* scholarship through 2004. Richard L. Hasen, *A Critical Guide to* Bush v. Gore *Scholarship*, 7 ANN. REV. POL. SCI. 297, 301–04 (2004).

[7] *E.g.*, Miriam Galston, *When Statutory Regimes Collide: Will* Citizens United *and* Wisconsin Right To Life *Make Federal Tax Regulation of Campaign Activity Unconstitutional*?, 13 U. PA. J. CONST. L. 867 (2011) (exploring the continuing viability of campaign finance regulation via tax law); Allison R. Hayward, *What Changes Do Recent Supreme Court Decisions Require For Federal Campaign Finance Statutes And Regulations?*, 44 IND. L. REV. 285 (2010) (examining recent Court rulings on the Federal Election Campaign Act and state statutes); Samuel Issacharoff, *On Political Corruption,* 124 HARV. L. REV. 118 (2010) (critically evaluating corruption as a justification for campaign finance regulation); Justin Levitt, *Confronting The Impact of* Citizens United*,* 29 YALE L. & POL'Y REV. 217 (2011) (reviewing the line of cases that led to *Citizens United* and contending that the notorious case was a small step from prior precedent); Richard Briffault, McConnell v. FEC *and the Transformation of Campaign Finance Law*, 3 ELECTION L.J. 147 (2004) (mapping the changes in campaign finance jurisprudence in the post-Clinton era).

[8] *E.g.*, Steven F. Huefner, *Don't Just Make Redistricters More Accountable to the People, Make Them the People,* 5 DUKE J. CONST. L. & PUB. POL'Y 37, 37 (2010) (discussing the "practical possibility of designing an apolitical redistricting process"); Samuel Issacharoff & Pamela S. Karlan, *Where to Draw the Line?: Judicial Review of Partisan Gerrymanders,* 153 U. PA. L. REV. 541, 555 (2004); Nathaniel Persily, *The Law of The Census: How to Count, What to Count, Whom to Count, and Where to Count Them*, 32 CARDOZO L. REV. 755 (2011) (providing

Election law scholars recognize that each of these constellations of issues offer rich opportunities for partisan gaming and tools for structurally insulating incumbents from meaningful election contests. As such, they pose serious risks to realizing the constitutional promise of popular sovereignty.[10] Yet, if each of these issues were resolved in a hypothetically ideal manner but the voting technology status quo remained uncorrected, the individual and aggregated right to vote would be seriously threatened, with federal elections potentially transformed into mere theatre.

This Article seeks to rally legal scholars with election law expertise to dedicate a portion of their considerable intellectual firepower to legal questions raised by problematic voting technologies. After minority undervote rates and disability accessibility issues appeared to have been solved, or at least far better managed by newer computer-based technologies,[11] almost all election

an overview of the laws regulating the census); Pildes, *supra* note 6, at 55–83; Michael J. Pitts, *Redistricting and Discriminatory Purpose*, 59 AM. U. L. REV. 1575, 1579 (2010) (proposing a new model for the Court to use when examining discrimination in the context of redistricting).

[9] *E.g.*, Christopher S. Elmendorf, *Undue Burdens on Voter Participation: New Pressures for a Structural Theory of the Right to Vote?,* 35 HASTINGS CONST. L.Q. 643, 644 (2008) (hypothesizing the Court will soon abandon its long–held "individual rights" and "no theory" precepts); Edward B. Foley & Bradley A. Smith, *Voter ID: What's At Stake?,* 156 U. PA. L. REV. PENNUMBRA 241 (2007); Justin Levitt, *Election Deform: The Pursuit of Unwarranted Electoral Regulation*, 11 ELECTION L.J. 97 (2012) (arguing new voter regulations are unwarranted and will re-open the gap between the demographics of those who vote and the population as a whole); Spencer Overton, *Voter Identification,* 105 MICH. L. REV. 631, 657–63 (2007) (exploring the scope and potential impact of photographic identification requirements for voting); Nathaniel Persily, *Fig Leaves and Tea Leaves in The Supreme Court's Recent Election Law Decisions,* 2008 SUP. CT. REV. 89 (2008); Daniel P. Tokaji, *Early Returns on Election Reform: Discretion, Disenfranchisement, and the Help America Vote Act,* 73 GEO. WASH. L. REV. 1206, 1233 (2005) (examining federal election administrative issues that resulted in disenfranchisement in Ohio and elsewhere, and the federal remedial statute); Hans A. von Spakovsky, *Protecting the Integrity of the Election Process,* 11 ELECTION L.J. 90 (2012) (arguing in favor of photographic identification requirements as an integrity component).

[10] Popular sovereignty is directly referenced in the Guarantee Clause, U.S. CONST. art. IV, § 4 (providing that "[t]he United States shall guarantee to every State in this Union a Republican Form of Government"). *See* AKHIL REED AMAR, AMERICA'S CONSTITUTION: A BIOGRAPHY 276–80 (2006) (explaining "the essence of the Article IV guarantee of each state's 'Republican' form of government" as "to shore up popular sovereignty"); Kathryn Abrams, *No "There" There: State Autonomy and Voting Rights Regulation*, 65 U. COLO. L. REV. 835 (1994) (explaining Guarantee Clause's interpretive meaning in the voting rights context); Michael W. McConnell, *The Redistricting Cases: Original Mistakes and Current Consequences*, 24 HARV. J.L. & PUB. POL'Y 103, 106–107 (2000) (contending the "Republican Form of Government Clause is a structural or institutional guarantee, emphasizing the right of 'the People'–the majority–to ultimate political authority."). One, therefore, might contend that the structural aspects of the right to vote are represented in the Guarantee Clause far better than the Equal Protection Clause. *See* Jesse H. Choper, *The Political Question Doctrine: Suggested Criteria,* 54 DUKE L.J. 1457, 1484 (2005) (suggesting that *Baker* "may be viewed as presenting a Guarantee Clause claim in disguise . . . .").

[11] *See* HAVA, *infra* notes 23, 27 (compelling "notice voting"). The Brennan Center for

legal scholars apparently lost interest in voting technology questions.[12] But the scientific studies raise new bases for questioning not only whether these underserved communities' needs are met by the deployed technologies, but also whether the well-meant electronic cure[13] for Floridian punch card irregularities has led to dramatically more serious legal issues.

The Supreme Court has frequently delineated the fundamental right to vote as including the right to have vote choices correctly recorded, counted as they were cast, and correctly reported in the final tally.[14] While its ballot box-stuffing cases repeatedly underscore these subsidiary steps as integral to the right to vote,[15] these cases and their principles generally do not surface in lower court opinions adjudicating the constitutional sufficiency of challenged e-voting technology. This omission warrants correction, and the principles thereby rescued will assist courts in applying the correct standard of review. If the constellation of voting systems and operating procedures permits covert, untraceable electronic ballot box-stuffing, the constitutional commitment is not realized and should be actionable under the Fourteenth Amendment Republic-protecting strict scrutiny review.[16]

Justice concluded that voting technology improvements post–HAVA had significantly reduced the undervote and overvote rates of minority voters. Press Release, Brennan Center for Justice, Brennan Center Report Finds Improvements in New Voting Technology Being Implemented in Several States (Aug. 28, 2006), *available at* http://www.brennancenter.org/content/resource/brennan_center_report_finds_improvements_in_new_voting_technology_being_imp. Whether voting participation barriers for voters with disabilities have been resolved is particularly disputed. The TTBR assessed the actual real-world success of supposedly accessible technologies for disabled voters and finding them lacking, *see infra* text accompanying notes 79–82.

[12] The few notable exceptions include election law scholars Richard Hasen, Heather Gerken, and Dan Tokaji. *See infra* notes 106, 113–15. In the allied field of political science, a Cal Tech/MIT Voting Technology Project scholar notes, "voting technology has been an orphan in political science since the creation of the profession, as it has also been for its sister profession, public administration. Lack of sustained research on voting technologies has paralleled lack of attention more generally to issues of election administration and its effects on election outcomes." Charles Stewart III, *Voting Technology,* 14 ANN. REV. POL. SCI. 353, 372 (2011). Election Law is obviously a third such field that has omitted sustained attention to election technologies.

[13] In this Article, "e-voting," "electronic voting" and "computer-based voting" are used interchangeably to embrace all types of computer-based voting systems. These include optical scanners, direct recording electronic (DRE) touchscreens, and Internet systems, and even embrace the discredited punch card systems.

[14] *See, e.g.,* Reynolds v. Sims, 377 U.S. 533, 554–55 (1964); Baker v. Carr, 369 U.S. 186, 208 (1962); United States v. Classic, 313 U.S. 299, 315 (1941).

[15] *See, e.g.,* Gray v. Sanders, 372 U.S. 368, 380 (1963) and cases *infra* note 87.

[16] Thus far, the Court has not combined an understanding of cyber security threats with the realities of current voting technologies.

My analysis seeks to underscore the gravity of technologically threatened constitutional voting rights and values, implicating both individual rights to vote and the structural promise of popular sovereignty. Resolution of the dispute over the meaning of Fourteenth Amendment[17] principles properly derived from *Bush v. Gore*[18] will be pivotal to assuring meaningful voting rights in the information society. If the Court should hold the Fourteenth Amendment to embrace a deferential standard of review or arduous intent requirements, allowing state political branches to persist in choosing voting technologies based on scientifically unfounded premises that do not achieve classic components of voting rights, the American Republic's future is seriously endangered.[19]

The argument proceeds in two parts. Part I traces illustrative empirical findings of the two comprehensive, definitive voting systems studies, offers evidence derived from actual election calamities that substantiates the experts' findings, and translates these findings into concepts meaningful for voting rights and election law. Part II considers the judiciary's failures thus far to understand the legal import of the scientific studies of voting systems when adjudicating the structural legal sufficiency of deployed voting systems[20] and identifies questions on which scholarship is critically needed. Throughout, owing to space constraints, the argument is illustrative rather than comprehensive.

[17] U.S. CONST. amend. XIV, § 1 (supporting Equal Protection and Substantive Due Process claims).

[18] 531 U.S. 98 (2000).

[19] Thus, this Article contends that courts' rulings in constitutional challenges to DREs that lacked a software-independent record of the voters' selections failed to understand the import of the security studies for the fundamental right to vote. Each of the earlier courts used a sliding scale or balancing test rather than strict scrutiny, and indulged a preference to defer to the political branches in the choice of voting systems. *E.g.*, Weber v. Shelley, 347 F.3d 1101, 1106 (9th Cir. 2003), Wexler v. Anderson, 452 F.3d 1226, 1232 (11th Cir. 2006), Tex. Democratic Party v. Williams, 285 F. App'x 194, 195 (5th Cir. 2008) (per curiam), *cert. denied,* 129 S. Ct. 912 (2009); Andrade v. NAACP of Austin, 345 S.W.3d 1,12 (Tex. 2011).

[20] Part II draws in part on the analytic approach and legal policy recommendations of three noted election legal scholars: Richard Hasen, Heather Gerken, and Dan Tokaji. Although their scholarly work to date has not responded to the comprehensive, definitive scientific studies of voting technology, these academics depart from the field's scholarly norm by characterizing voting technology as a central problem for election law and voting rights. My future work will draw on Hasen, Gerken, and Tokaji in greater depth. Owing to space constraints, this Article limits its concern to structural constitutional litigation external to an election contest. Hence, it does not directly consider candidate challenges to counts or claims for recounts.

I. The Scientific and Performance Record Relevant to the Constitutional Sufficiency of Deployed Voting Systems

Problematic voting devices that produced ambiguous vote totals and inconsistent recounts famously triggered the U.S. Supreme Court's intercession into Florida's 2000 presidential election tabulation.[21] In response to *Bush v. Gore*[22] and the resulting public furor, Congress passed the Help America Vote Act of 2002 ("HAVA").[23] Its statutory standards requiring that voters be allowed to correct balloting errors before casting a ballot virtually mandated the replacement of existing voting devices with new computer-based voting.[24] Most states moved from punch cards or lever systems in 2004–05 after receiving an allotment from the $3 billion in federal monies designed to incentivize the change.[25] The first scientific assessments of the software and security features in the new voting systems that were conducted independent of the manufacturers occurred in 2003 and 2004.[26] In 2007, after the earlier studies had identified grave deficiencies, the California and Ohio Secretaries of State convened definitive, multi-system studies with teams of prominent computer scientists and other experts from across the nation. This Part briefly reviews the findings in these two major studies and offers some illustrative examples of how these documented flaws affect real elections.

A. The Comprehensive, Definitive Voting Systems Reviews

HAVA provided substantial financial incentives for states to replace their existing punch card and lever voting systems, but it required new systems to satisfy specified functional criteria.[27] These

[21] 531 U.S. 98 (2000).

[22] *Id.*

[23] The Help America Vote Act of 2002, 42 U.S.C. §§ 15301–15545 (2006) [hereinafter HAVA].

[24] HAVA § 15481(a)(1)(A). The punch card systems were not simply mechanical but also included computer components. *See* ROY G. SALTMAN, THE HISTORY AND POLITICS OF VOTING TECHNOLOGY: IN QUEST OF INTEGRITY AND PUBLIC CONFIDENCE 160–69 (2006).

[25] *See* HAVA §§ 15301–05 (authorizing payments to State governments); Tova Wang, *Competing Values or False Choices: Coming to Consensus on the Election Reform Debate in Washington State and the Country*, 29 SEATTLE U.L. REV 353, 355 (2005) (reporting that $3.1 billion had been allocated to states for election improvements by 2005).

[26] In 2003, the Ohio Secretary of State contracted with consultant Compuware to assess the four major vendors' DRE touchscreen voting systems. *See* COMPUWARE CORPORATION, DIRECT RECORDING ELECTRONIC ("DRE") TECHNICAL SECURITY ASSESSMENT REPORT (2003) [hereinafter COMPUWARE] (publishing the public report). The Maryland legislature convened the RABA scientific study. RABA TECHNOLOGIES, LLC, TRUSTED AGENT REPORT: DIEBOLD ACCUVOTE-TS VOTING SYSTEM (2004) [hereinafter RABA study].

[27] HAVA's § 15302 mandates voting system compliance with functional specifications

requirements included provision of notice to the voter of errors such as "overvoting" a race by marking too many choices,[28] so that the voter might correct any errors before the ballot is cast. To satisfy notice or "second chance" voting and other requirements, HAVA led states to authorize purchases of three kinds of voting systems:[29] optical scanners for reading paper ballots,[30] direct recording electronic ("DRE") machines that normally offer a touch screen for marking electronic ballot choices, and computerized ballot-marking devices designed primarily for disability access. Each system's software generates the electronic ballot "styles" or "definitions"[31] by assembling the election data so that it can be printed (for optical scan ballots) or copied to memory media for display on DRE voting devices.[32] The software later tabulates and reports the election totals from both types of voting devices into one election results report.

California's Secretary of State, Debra Bowen, contracted the Top to Bottom Review ("TTBR") to the University of California shortly after she was inaugurated in 2007. The project was led and staffed by nationally recognized computer scientists, of whom a number of had amassed high-profile voting systems forensic experience in problematic elections. The TTBR evaluated three proprietary voting systems—Diebold, Hart, and Sequoia systems—that were deployed not only in California, but also nationwide with only minor differences.[33] Its scientists discovered both serious engineering and coding errors (software "bugs") as well as security design and coding

that include those detailed in § 15481(a)(1)(A), requiring an opportunity for voter verification of ballot choices before the ballot is cast, and an opportunity to change ballot choices and be notified of any overvotes, with an option to correct the ballot before it is cast. The mandatory minimum statutory standards for voting systems also specify a manual audit capacity on a permanent paper record, § 15481(a)(2)(B), and the maximum error rate permitted by a voting system, § 15481(a)(5)(B).

[28] HAVA § 15481(a)(1)(A)(iii).

[29] HAVA defines a "voting system" at § 15481(b) in expansive terms.

[30] Optical scanners include portable, low-capacity, precinct-based models and high-speed, high-capacity, centralized scanning units.

[31] In some states, such as Ohio, ballot rotation rules produce the need for a different ballot in every precinct. *See* CUYAHOGA ELECTION REVIEW PANEL: FINAL REPORT (2006) (reporting that the county required almost 7,000 separate ballot styles in the failed election). In federal primaries, ballot rotation and separate party ballots can lead to five or more ballot styles per precinct, placing a huge burden on staff.

[32] A DRE is a voting unit that digitally records voters' choices. The current generation of DREs tends to feature a touch screen 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 each voter's choices. Some DREs print an "audit trail" on spooled paper.

[33] The TTBR did not review the ES&S systems, but California convened a different review. *See* TTBR, *supra* note 2 (linking to ES&S material under the Election Systems and Software heading).

errors, all of which can manifest in reporting false vote tallies or in rendering the system unavailable for voters' use.[34]

Software constitutes a critical component of these digital election systems. It provides instructions to a computer that include delineation of the functions to perform, their order of operation, what audit logs will be maintained, and many others. In a database program like that used in voting systems, software creates the "buckets" within which votes will be "deposited" or recorded in humanly unreadable language. The buckets for each candidate and question on the ballot must be properly mapped to a "button" or an oval that the voter uses to identify vote choices. The voter's selections must be translated by a chain of electronic interactions into records kept in electronic buckets, which are thereafter copied and interpreted by a chain of additional electronic transactions until ultimately reported as cast vote reports in humanly comprehensible language. Computer science and engineering experts stress that election officials and voters have no method by which to determine whether all steps in this electronic chain have been completed correctly.[35] The accountability functionality available through automatic logging can assist in identifying transaction errors if engineered appropriately, but would require the systems' designs to incorporate rigorous monitoring and self-reporting of errors, and also protections for the auditing functions so their data cannot be erased or disabled.[36] The content of the

[34] Bugs can introduce system instability and failures, also known as "access" issues, in addition to security issues. *See, e.g.*, Matt Blaze et al., *Source Code Review of the Sequoia Voting System* 33, 41 (2007), http://www.sos.ca.gov/voting-systems/oversight/ttbr/sequoia-source-public-jul26.pdf (noting that "[c]omplex software systems are especially susceptible to bugs or errors that cause the system to behave in an unintended manner. When one of these bugs is encountered, the effect can vary from causing minor instability to enabling devastating security exploits . . . . [Exacerbations of software bugs] will be detrimental to the system's reliability and usability").

[35] *See, e.g.*, Thomas Ryan and Candice Hoke, *GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standard*s, in PROCEEDINGS OF THE USENIX/ACCURATE ELECTRONIC VOTING TECHNOLOGY WORKSHOP (2007) (reporting design and engineering errors that can affect the accuracy of election results). Both TTBR and EVEREST confirmed the conclusions of this paper. EVEREST: EVALUATION AND VALIDATION OF ELECTION-RELATED EQUIPMENT, STANDARDS, AND TESTING § 13.1.1 (2007) [hereinafter EVEREST FINAL REPORT]; UNIVERSITY OF CALIFORNIA-BERKELEY, SOURCE CODE REVIEW OF THE DIEBOLD VOTING SYSTEM § 5.3.1 (2007), *available at* http://www.sos.ca.gov/voting-systems/oversight/ttbr/diebold-source-public-jul29.pdf [hereinafter UC SOURCE CODE REVIEW]. While no feasible method allows election officials and voters to ascertain the correctness of each component step in the electronic cascade of e-voting system communication, robust post-election auditing permits effective checks on the final results—which may suffice for the critical needs of election officials and voters. *See infra* text accompanying notes 156–63.

[36] Election officials in Humboldt County, California, discovered a logging design failure in the Diebold GEMS tabulation software when physical ballot totals did not match the software record. The officials found that the audit log failed to provide a record of ballot batch files that the officials had deleted when they suspected an error. Kim Zetter, *Serious Error in Diebold Voting Software Caused Lost Ballots in California County–Update,* WIRED (Dec. 8, 2008, 2:32

automatic logging must also be designed not to contain data that could compromise the anonymity and secrecy of the ballot.

Software "bugs" or coding errors and engineering choices can be analyzed separately with regard to performance stability and functionality. Serious bugs can result in a failure of the system to function correctly, or at all. As the Sequoia examiners wrote: "Complex software systems are especially susceptible to bugs or errors that cause the system to behave in an unintended manner. When one of these bugs is encountered, the effect can vary from causing minor instability to enabling devastating security exploits."[37]

The most troubling security flaws TTBR researchers discovered lay at the level of baseline, elementary computer security. These mistakes were blatant violations of the most settled, foundational principles of security software design and "robust" programming. The researchers concluded that the software of all systems lacked basic security protections. All systems failed to follow standard security design principles. All systems were susceptible to viruses that could be introduced from a number of vectors, including from voting device memory cards. These design defects offered hundreds (if not thousands) of different opportunities in every election for inserting programming code that would "flip" votes among candidates, scramble tabulation data, delete voting data, provide "back doors" for remote tampering, or cause system programming to fail.[38]

Information systems design precepts for vital data where accuracy and security rank as preeminent objectives include structuring and rigorously protecting audit logs so they will automatically record all operator activity. In the election context, this design feature would allow for the monitoring of all tabulation activity, including any effort to delete or substitute vote data. HAVA specifies that voting systems shall have an "audit capacity" without supplying details of the

PM), http://www.wired.com/threatlevel/2008/12/unique-election/. Zetter quotes a software specialist: "This means the audit log is not truly a 'log' in the classical computer program sense, but is rather a 're-imagining' of what GEMS would like the audit log to be, based on whatever information GEMS happens to remember at the end of the vote counting process." *Id.* After the election officials reported the problem to the California Secretary of State, the vendor summarily terminated its contract with the county. *See* Parke Bostrom, *Disclosed: Diebold/Premier's Humboldt County Termination Letters*, THE BRAD BLOG (Apr. 30, 2009, 4:32 PM), http://www.bradblog.com/?p=7109#more-7109 (displaying the Diebold contract termination letters).

[37] Blaze et al*., supra* note 34, at 33.

[38] *See UC Source Code Team Reports & UC Red Team Reports for Diebold/Premier, Sequoia, and Hart InterCivic*, TTBR, *supra* note 2, (documenting the final reports from the University of California scientists detailing their findings from the top-to-bottom review).

required features.[39] Perhaps not surprisingly, the studies found that the voting systems' logs that recorded operator activity had failed to satisfy industry standard design protections to prevent their accidental or intentional overwriting or erasure.[40] In a banking environment, logs constitute records that will "report" attempts to transfer funds and thus act as a deterrent of illegal conduct. In the voting arena, failure to protect the logs means that motivated "insiders" could manipulate voting data and results, and then erase the log inventories that would show their identity and activity inside the tabulation database. Or, the opportunity could be used to frame a different employee for nefarious conduct.

All voting systems' "election management" software failed to maintain minimally adequate system access controls, as they permitted relatively easy bypassing of passwords. Many other security holes existed in each system that easily permitted the voting system to be compromised in ways that could prevent the system's ability to report accurate election results—or any results.

The TTBR also included an expert accessibility team[41] strictly dedicated to assessing all three voting systems for their usability and accessibility for voters with physical disabilities or alternate language needs.[42] Although vendors marketed many of these DRE systems as satisfying legal requirements for physical accessibility, usability

[39] HAVA § 15481(a)(2).

[40] Some of the Diebold/Premier voting systems not only lacked protection of audit logs but also provided a "clear" button for permanently erasing the audit log. *See* Kim Zetter, *Report: Diebold Voting System Has 'Delete' Button for Erasing Audit Logs,* WIRED, (Mar. 3, 2009, 4:30 PM), http://www.wired.com/threatlevel/2009/03/ca-report-finds (reporting on the California Secretary of State's investigation and conclusion that the button violates HAVA: "the Clear buttons … allow inadvertent or malicious destruction of critical audit trail records in all Gems version 1.18.19 jurisdictions, risking the accuracy and integrity of elections conducted using this voting system").

[41] The California Secretary of State described the accessibility consultants:

> The accessibility of the voting systems will be assessed by a single team of two accessibility experts, headed by Noel Runyan of Campbell, California. Mr. Runyan is an electrical engineer and computer scientist with over 33 years experience in design and manufacturing of access technology systems for people with disabilities. For the last four years, he has concentrated on the accessibility of voting systems. The accessibility assessment will include test voting on each of the voting systems by volunteer voters representing a broad range of disabilities.

News Release, Debra Bowen California Secretary of State, Frequently Asked Questions About Secretary of State Debra Bowen's Top–To–Bottom Review of California's Voting System (June 13, 2007), http://www.sos.ca.gov/voting-systems/oversight/ttbr/ttbr-q-and-a-061307.pdf.

[42] NOEL RUNYAN AND JIM TOBIAS, ACCESSIBILITY REVIEW REPORT FOR CALIFORNIA TOP–TO–BOTTOM VOTING SYSTEMS REVIEW 1 (2007) (explaining that the authors evaluated "usability and accessibility for voters with disabilities and voters with alternate language needs, using both heuristic and user testing techniques").

testing demonstrated that the DRE systems could not accommodate most individuals with disabilities.[43] For instance, physical access by wheelchair-bound individuals could often not be achieved because of design features.[44] Audio ballot functions for visually impaired voters proved unwieldy for the target voters.[45] The authors concluded that "none met the accessibility requirements of current law and none performed satisfactorily in test voting by persons with a range of disabilities and alternate language needs."[46] The California Secretary of State responded by mandating many managerial and technical modifications to the DREs as a condition of their continued use.[47] Recalling that these same DREs are widely deployed nationwide under the presumption they satisfy requirements for "accessible" voting systems, the larger legal question may be why no litigation or other decertification proceedings have occurred elsewhere. Developing these crucial legal underpinnings is a task needing the assistance of election law scholars concerned with underserved communities.[48]

After publication of the TTBR reports in August, the Ohio EVEREST study commenced, with most work occurring during the fall of 2007.[49] Its methodology differed somewhat in that the state

[43] *Id.* Fortunately, the experts were able to generate a list of modifications ("mitigations") that could allow the systems to become accessible and fully usable to most of the targeted voters, but configured as marketed, they legally failed compliance assessments. *Id.* at 30–35. The experts wrote they could describe "possible improvements to the concerns . . . . All of these options are actions that could readily be taken by poll workers or other election officials, or by manufacturers, using materials and techniques we believe they may have at hand." *Id* at 30.

[44] *Id.* at 6–12.

[45] *Id.* at 20–23.

[46] *Id.* at 1.

[47] The Secretary's DRE orders predominantly focused on narrowing the security gaps and reducing the number of voters who would cast ballots on these devices. She also required a 100 percent hand recount of all ballots cast on the DREs, using the VVPAT (Voter-Verified Paper Audit Trail) in separate orders addressed to each voting system. *See, e.g.*, STATE OF CALIFORNIA, SECRETARY OF STATE, WITHDRAWAL OF APPROVAL OF DIEBOLD ELECTION SYSTEMS, INC., GEMS .18.24/ACCUVOTE-TSWACCUVOTE-OS DRE & OPTICAL SCAN VOTING SYSTEM AND CONDITIONAL RE-APPROVAL OF USE OF DIEBOLD ELECTION SYSTEMS, INC., GEMS 1.18.24/ACCUVOTE-TSX/ACCUVOTE-OS DRE & OPTICAL SCAN VOTING SYSTEM 5 (2007) (specifying that "[t]he jurisdiction must conduct a 100% manual tally, by the process described in Elections Code section 15360, of all votes cast on an AccuVote-TSx [Diebold DRE]").

[48] Two Ohio State University legal scholars have shown significant interest in accessible voting, *see* Daniel P. Tokaji & Ruth Colker, *Absentee Voting by People with Disabilities: Promoting Access and Integrity*, 38 MCGEORGE L. REV. 1015 (2007). But their article's scope excludes precinct-based voting. Tokaji addressed these questions in a separate article that preceded the TTBR's findings. Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711 (2005).

[49] A number of the TTBR scientists, including team leaders Matt Blaze and Giovanni Vigna, also led parts of the EVEREST work but under slightly different contractual arrangements and with a substantially lengthier research period. EVEREST could thus effectively build upon the TTBR. *See* EVEREST FINAL REPORT, *supra* note 35 (explaining that

contract convened three separate teams from different sectors: one academic team,[50] one private security consultant firm,[51] and one voting system testing laboratory.[52] One key contribution lay in its comprehensive evaluation of the ES&S voting systems.[53] A second difference lay in the security consulting firm's development of a yardstick or grading metric of twelve criteria that reflected the industry's standard best practices where security was a major objective; the firm scored each voting system with simply a pass or fail on each criterion.[54]

Like the TTBR, EVEREST identified systematically a wide range of defects and vulnerabilities that could be used to subvert accurate election counts in undetectable and untraceable ways.[55] They found this conclusion valid for ES&S's voting system as well, which had been omitted from the TTBR assessments. The EVEREST teams discovered that ES&S voting systems paralleled other vendors for they had not been designed in accordance with industry standards for data accuracy and security, and lacked both robust code and compliance with accessibility standards. The researchers underscored that ES&S systems could not be distinguished from the other problematic voting systems, "exhibited a visible lack of trustworthy

the analyses were conducted between October 1, 2007 and December 7, 2007, and listing Matt Blaze and Giovanni Vigna as team leaders). This author assisted the Ohio Secretary of State's office and the academic teams in planning the studies and in educating the researchers on election law and processes.

[50] The EVEREST academic team's leadership was provided by Professor Patrick McDaniel of Pennsylvania State University. *Id.*

[51] MicroSolved, Inc., of Columbus, Ohio, conducted a broad range of security assessments. *See* OHIO SEC'Y OF STATE, EVEREST PROJECT, ES&S SYSTEM MICROSOLVED, INC. EXECUTIVE SUMMARY REPORT (2007) (examining the security of the electronic voting systems in Ohio).

[52] Certified as a voting system testing laboratory, SysTest Labs conducted an assessment of eleven counties' written security policies but did not assess compliance with policies in real elections, as had originally been envisioned. *See* STATE OF OHIO, SEC'Y OF STATE, CONSULTING AND TESTING SERVICES RISK ASSESSMENT STUDY OF OHIO VOTING SYSTEMS, EXECUTIVE SUMMARY (2007) (assessing State of Ohio certified voting systems) and author's planning notes (on file with author).

[53] *See* EVEREST FINAL REPORT, *supra* note 35, at 27–98 (evaluating the ability of the ES&S voting systems to conduct trustworthy elections). Corporate delay tactics had successfully excluded the ES&S systems from TTBR review. Despite receiving commitments to participate in the TTBR from all four vendors of California-certified voting systems, only three (Sequoia, Diebold (now Dominion), and Hart InterCivic) complied with the project's calendar sufficiently to be reviewed. *See* TTBR, *supra* note 2 (listing the voting systems that were reviewed and providing links to the reviews).

[54] OHIO SEC'Y OF STATE, JENNIFER L. BRUNNER, PROJECT EVEREST: EVALUATION AND VALIDATION OF ELECTION RELATED EQUIPMENT, STANDARDS AND TESTING 15 (2007) [hereinafter EVEREST EXECUTIVE REPORT].

[55] *See* EVEREST FINAL REPORT, *supra* note 35, at 3–4 (describing the security failures present in the studied systems).

auditing capability."[56] Activity logs could easily be forged or erased by those individuals whose activity was "intended to be monitor[ed]," with the cumulative import that "it is difficult to know when an attack occurs, or to know how to isolate or recover from it when it is detected."[57]

EVEREST and TTBR thus clarified and reinforced four critical points germane to evaluating the legal sufficiency of deployed voting systems. All of the voting systems that are in wide deployment nationally are pervaded with software design and coding errors that can randomly cause vote loss, miscounts, or other voting device malfunctions. In legal terms, they can function in an arbitrary and capricious manner with no demonstrable evidence of such errors.[58] Second, all of the systems pervasively provide opportunities for deliberate covert tampering with all aspects of an election's processes, including the tabulation reports of winners and losers; these intrusions can also be achieved by remote connections.[59] Third, all systems afford efficient and relatively complete ways for a motivated individual to cover one's tracks by deleting or modifying the logs, thus additionally providing a relatively effective cover for nefarious activities. Fourth, mitigations cannot be devised to eliminate all or most of the opportunities to tamper; the failure of designing for security at the outset cannot be overcome by managerial practices or software patches.[60]

This conclusion that the deployed voting system software has not been engineered to and cannot consistently and reliably achieve high accuracy in core functions finds additional support from the "twelve-step baseline comparison framework" of the industry standard best practices. When measured against these twelve basic standards, the

[56] *Id.* at 3.

[57] *Id.*

[58] Consider the Court's comment in *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." While computer forensic experts may be able to determine whether errors occurred and with what impact on vote recording or tallies, most election officials lack such expertise.

[59] The 2011 Venango County, PA forensic audit found that an unauthorized remote connection to the ES&S tabulation sever occurred multiple times in the election cycle, a connection that was unknown and unreported to the election officials until the forensic specialists filed their report. *See* David A. Eckhardt, *Audit Analysis of the Venango County 2011 Municipal Primary* 15 (2011), http://bradblog.com/Docs/VenangoCounty_InitialReport_DavidEckhardt_111511.pdf (discussing the use of a remote-access application).

[60] See *infra* text accompanying note 156–63 for discussion of a methodology that allows cost-effective, feasible checks on vote totals (external to evaluating the correctness or integrity of software code), and strong possibilities for reconstructing accurate totals despite bug-infected or deliberately modified vote totals. These rigorous auditing approaches can thus permit aging, , problematic voting systems to continue to be deployed rather than replaced.

EVEREST professional security consultants discovered that all of the voting systems fell well below reasonable engineering expectations. They concluded Premier and Hart InterCivic "scored a 'zero,'" that is, the Premier and Hart InterCivic voting systems "failed to meet any of the twelve basic best practices requirements."[61] ES&S scored one out of twelve points.[62] Qualified security experts, with knowledge of both the industry's engineering standards and the tools for diagnosing problems, have engaged in comprehensive evaluations of electronic voting systems; they have counseled the public and election officials that without other corrections and quality assurance steps,[63] these machines are unfit for voting.

The TTBR Red Team Summary unequivocally concluded their testing had "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."[64] 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*."[65] These conclusions underscore that the vote totals may be accurate—or may be partially or grossly inaccurate—because the systems' core operations may be impaired by software bugs, deliberate tampering, or inadvertent errors at any of multiple levels.

When the TTBR and EVEREST studies were published, voting system vendors (joined by some election officials) sought to dismiss the scientific findings as contrived in an ivory tower laboratory setting remote from real world conditions.[66] As the next section addresses, the vendors also advanced the empirically false claim that

[61] EVEREST EXECUTIVE REPORT, *supra* note 54, at 22, 32.

[62] *Id.* at 28.

[63] *See infra* text accompanying notes 156–57, for a discussion of how voting equipment that is controlled by flawed software can still be used to achieve accurate election results; *see also* P.B. Stark & D.A. Wagner, *Evidence–Based Elections* 6 (forthcoming Oct. 2012), *available at* http://statistics.berkeley.edu/~stark/Preprints/evidenceVote12.pdf (arguing for the use of software-independent voting systems and robust post-election audits).

[64] MATT BISHOP, OVERVIEW OF RED TEAM REPORTS (emphasis added).

[65] EVEREST FINAL REPORT, *supra* note 35, at 3 (emphasis added).

[66] *See, e.g.*, Letter from Steve Weir, President, Cal. Assoc. of Clerks and Election Officials, to Top-to-Bottom Review Pub. Hearing (July 30, 2007), *available at* http://www.sos.ca.gov/voting-systems/oversight/ttbr/archive/comments/caceo.pdf (criticizing the testing used in the Top-to-Bottom Review); Press Release, Sequoia Voting Sys., Response from Sequoia Voting Sys. to the Cal. Sec'y of State's Office on the Top-to-Bottom Review of Voting Sys. (July 30, 2007), *available at* http://www.sos.ca.gov/voting-systems/oversight/ttbr/archive/comments/sequoia.pdf (arguing that the Top–to–Bottom Review suffered from faulty methodology); Press Release, Premier Election Solutions, Premier Technical Response to the Ohio Everest Report (Mar. 2008), *available at* http://www.sos.state.oh.us/SOS/upload/everest/premierResponse.pdf (criticizing the EVEREST study's approach).

no proof had established any successful attacks against an electronic voting system.[67] The vendors did not disclose, however, that their procurement contracts routinely included clauses barring independent forensic assessments of election databases and the voting equipment, and that many claimed proprietary ownership of the election data that had been processed by their software.[68] Thus, the vendors have

[67] A spokesperson for the Premier/Diebold system responded to EVEREST, claiming, "It is important to note . . . that there has not been a single documented case of a successful attack against an electronic voting system, in Ohio or anywhere in the United States." Bob Driehaus, *Ohio Elections Official Calls Machines Flawed*, N.Y. TIMES, Dec. 15, 2007, at A14.

While the vendors and many election officials repeated this claim of no successful attack, it arguably is false. As just one example, in the 2006 general election, the Public Monitor of Cuyahoga Election Reform (appointed by the Cuyahoga County Board of Elections and the County Commissioners) collected substantial circumstantial evidence of malfeasance in the Board of Elections (BOE). *See* Memorandum from Candice Hoke, CSU Ctr. for Election Integrity, to the Cuyahoga Cnty. Bd. of Elections Bd. Members 9–20 (Jan. 8, 2007), *available at* http://www.urban.csuohio.edu/cei/public_monitor/Monitor-CCBOELegalCompliance1-8-07-MEMO-FINAL.pdf (identifying areas of legal noncompliance). Specifically, after the BOE spent two days scanning absentee ballots, a cable to the tabulation server that had been disconnected (as required by the security policy) mysteriously was re-connected after the server room had been locked and the personnel had supposedly left the building for the evening. The Windows event logs and the Diebold GEMS security logs reflecting this overnight period (when the room supposedly had been locked) suddenly did not match. The system clock inexplicably gained eleven hours; the Windows logs showed seven print commands of the absentee ballot tabulations in the off-hours, before Election Day and thus were arguably illegal. All BOE personnel accessing the server used an undifferentiated "admin" default password in violation of the security policy, which eliminated the capacity to track individual activity at the server or from a remote location. The Monitor commented:

> [T]he prohibition on generating reports of absentee voting results prior to the close of the polls on election day [rests in concerns that] early access to absentee vote tabulations could be used to compromise the fairness and results of the voting on election day. For instance, absentee voting results could be used to determine which precincts to disrupt on Election Day or to steer other forms of tampering. This concern is especially acute where the proportion of the votes cast by absentee ballot is extremely high, such as was the case in the November, 2006 election in which nearly 25% of votes were cast via absentee ballot.

Id. at 13 (as full disclosure, this author served as Project Director of the Monitor and wrote the report quoted above); *see also* Motion for Reconsideration, In re Venango Cnty. Election Bd., No. 219–2011 (Pa. Ct. Com. Pl. Dec. 2, 2011) (requesting continuation of forensic audit into Unity/ES&S election tabulation irregularities that included multiple candidates with zero votes and the presence of a program that permitted remote computers to log into the tabulation server that had been used multiple times in periods near election tabulations—a profound and heretofore hidden access point that could have eviscerated the county voters' election choices). David Eckhardt's preliminary forensic report reviews the methodology and evidence obtained. Eckhardt, *supra* note 59; *see also* Brad Friedman, *Special Report: Forensic Analysis Finds Venango County, Pa E-Voting System "Remotely Accessed" on "Multiple Occasions" by Unknown Computer*, THE BRAD BLOG (Dec. 12, 2011, 2:11 PM), http://www.bradblog.com/?p=8986#more-8986 (reporting background events and vendor ES&S's efforts to stop the forensic review). In 2010, the Libertarian Party challenged the structural lack of transparency and accountability of the local election office and its alleged use of Diebold software to tamper with election results. The Party won the right to proceed to trial on its claims. Ford v. Pima Cnty. Comm. of the Ariz. Libertarian Party, Inc., No. 2 CA–CV 2010–0001, 2010 WL 4296642 (Ariz. App. Div. Oct. 28, 2010).

[68] *See* Jennifer Nou, Note, *Privatizing Democracy: Promoting Election Integrity Through*

sought to clamp an iron cover of contractual legal prohibitions to bar public investigation of anomalies and irregularities. Vendors have routinely threatened lawsuits against election jurisdictions or county governments for violation of alleged proprietary and contractual rights when the election officials simply seek to ascertain the correct vote tallies from ambiguous or questionable tabulation reports.[69] The vendors thus use the clauses to eliminate the risk that evidence will be generated that can contradict the marketing assurances that the systems function accurately in real elections. Such evidence would potentially support claims of product defect or noncompliance with governing legal standards for election accuracy.

Because no federal agency collects voting system "incidents" and malfunction reports[70] and state governments generally do not assume

Procurement Contracts, 118 YALE L.J. 744, 781 (2009) (citing Diebold's argument that its software constituted a trade secret and could not be accessed by the board of elections); Joseph Lorenzo Hall, *Contractual Barriers to Transparency in Electronic Voting* (2007), http://static.usenix.org/events/evt07/tech/full_papers/hall/hall.pdf (explaining that voting system contracts restrict analysis and contain confidentiality provisions).

[69] The Diebold Corporation claimed that the Public Monitor's review of the database to ascertain corruption was prohibited by its contract with Cuyahoga County. But the Monitor prevailed, as a duly appointed agent of the County. *See* COLLABORATIVE PUBLIC AUDIT OF THE NOVEMBER 2006 GENERAL ELECTION 34–36, 66–67 (2007) (discussing the difficulties faced with obtaining the necessary files). More recently, ES&S threatened to sue Venango County for convening a forensic assessment of election anomalies. *See* Luther Weeks, *Voting Machine Investigation Leads to Serious Issues and Cover-Up*, CTVOTERSCOUNT (Dec. 19, 2011), http://www.ctvoterscount.org/painvestigation/ (explaining that ES&S is suing investigators); *Forensic Analysis Finds Venango County E–Voting System "Remotely Accessed" on "Multiple Occasions" by Unknown Computer*, THE VOTING NEWS (Dec. 13, 2011), http://thevotingnews.com/blogs/forensic-analysis-finds-venango-county-pennsylvania-e-voting-system-remotely-accessed-on-multiple-occasions-by-unknown-computer-the-brad-blog/ (discussing ES&S's threats to sue).

[70] The U.S. Election Assistance Commission has the jurisdiction, the power and arguably the duty, to generate an "incident" inventory. *See* HAVA § 15322 (2006) (describing the duties of the Election Assistance Commission). HAVA transferred the FEC informational clearinghouse duties to the EAC, including the reports function regarding voting systems performance. *See id.* (incorporating by reference the duties of HAVA §§ 15361–15387 (2006)). Whether the EAC holds clearinghouse duties to gather and post information regarding the performance of voting systems that lack EAC certification has been disputed. At a hearing on Dec. 8, 2008, the EAC heard oral testimony and received written statements regarding its clearinghouse powers and duty regarding these systems. *See* U.S. Election Assistance Comm'n, *Minutes of the Public Meeting* (2008), http://www.eac.gov/assets/1/AssetManager/transcript%20public%20meeting%20december%208%2020081.pdf (transcribing the testimony and statements regarding the EAC's powers). HAVA expressly confers EAC authority, and arguably a statutory duty, to provide voting systems informational (clearinghouse) reporting on voting systems that pre–date the EAC's certification system. *See* HAVA § 15371 (2006) (providing the EAC with the authority to certify and test voting systems). In § 15362(e), HAVA provides that the 2002 FEC standards "shall be deemed to have been adopted by the Commission as of" the date HAVA is enacted. *Id.* at § 15362(e). Hence, the FEC standards are now EAC standards, and the clearinghouse reporting duties encompass pre–EAC and post–EAC voting systems.

But the EAC has taken the position that its Quality Monitoring Program will collect this task, media reports have become the major source of documentation of flawed performance.

B. Field Experience of Problematic Voting Systems

Relatively unknown by the American voting public, a substantial empirical record demonstrates that the TTBR and EVEREST reports accurately predicted the inability of the voting systems to function reliably in generating consistently accurate tallies.[71] Deployed voting systems have produced negative numbers of votes cast,[72] failed to activate at the polls,[73] and permitted the concealed mismatching of candidates to bubbles or buttons,[74] resulting in "flipping" votes between candidates.[75] Without provocation or human error the systems have, for instance, counted some ballot batches or precincts multiple times[76] or produced vote tallies reflecting 3–5 times more ballots than participating voters.[77]

incidents and indicators of anomalies and malfunctions only for voting systems that have been tested in EAC-NIST certified labs and that have earned an EAC-certification for satisfying the Voluntary Voting System Guidelines (VVSG). *See Quality Monitoring Program*, U.S. ELECTION ASSISTANCE COMM'N, http://www.eac.gov/testing_and_certification/quality_monitoring_program.aspx (last visited May 10, 2012) (explaining that the EAC issues advisories for anomalies with EAC-certified systems). The EAC opines: "System Advisory Notices are an important part of the Quality Monitoring Program. EAC issues advisories to inform jurisdictions and members of the public of an existing anomaly or issue with an EAC-certified system." *Id.*

The agency relented somewhat and permits State and local election officials to file voting systems studies and reports which the EAC posts on its website. *See Voting Systems Reports Collection*, U.S. ELECTION ASSISTANCE COMM'N, http://www.eac.gov/testing_and_certification/voting_system_reports.aspx (last visited May 10, 2012) (providing voting system reports and studies conducted by state and local governments). The Brennan Center has offered an alternative "database inventor" approach in its recent report. *See* LAWRENCE NORDEN, VOTING SYSTEM FAILURES: A DATABASE SOLUTION 27–32 (2010) (proposing a publicly available, searchable centralized database).

[71] A partial inventory of miscounts in real elections has been produced by Common Cause & VotersUnite!. *A Master List of 70+ Voting Machine Failures and Miscounts by State*, COMMON CAUSE, http://www.commoncause.org/atf/cf/%7Bfb3c17e2-cdd1-4df6-92be-bd4429893665%7D/MASTERLISTOFMACHINEFAILURES.PDF (last visited May 10, 2012).

In 2009, VotersUnite! extended its study to errors committed attributable to ballot scanning technology, to demonstrate that these devices are not panaceas but equally afflicted with buggy software and security failings. Scanners do, however, offer one critical difference: a voter-marked paper ballot that can be re-tabulated by hand or by a validated scanner. *See* ELLEN THEISEN, BALLOT–SCANNER VOTING SYSTEM FAILURES IN THE NEWS—A PARTIAL LIST (2009) (tracking malfunctions of ballot-scanner systems); NORDEN, *supra* note 70, at 46–96 (collecting incidents of miscounts in Appendix B).

[72] *See* NORDEN, *supra* note 70, at 14 (citing 16,000 negative votes being recorded in one county).

[73] *See id.* at 16 (explaining that hundreds of polling sites had to delay opening their doors).

[74] *Id.* at 88–89, 94–95.

[75] *Id.*

[76] *Id.* at 21, 55, 87.

[77] *See* THEISEN, *supra* note 71, at 4, 38 (noting discrepancies between the number of

While optical scanners generate a voter-marked paper ballot, these systems are not foolproof in part because they use the same flawed central tabulating software as DREs. One nonprofit study reported in 2009:

> Despite historical evidence of scanner miscounts, results generated by ballot-scanner systems are rarely verified by a hand count unless the results appear implausible. Virtually all the miscounts described [in this report of over one hundred events] were detected by hand counting ballots when scanners produced implausible results. In some cases, erroneous results were certified because they appeared plausible and the error was discovered only after certification.[78]

With fewer than half the states conducting rigorous post-election audits to ascertain election tally accuracy, and fiscal pressures not to undertake "unessential" or new work, tabulation vote reports will generally not be reassessed in the absence of blatant improbability.

C. Research Conclusions with Import for Voting Rights and Election Law

Information systems are designed to fulfill particular hierarchies of functions and attributes, and must trade-off some capacities to achieve higher ranked objectives. Many operational contexts do not share with public elections the same critical need for high assurance of accuracy, security, and reliability. But Election Day and early voting are highly circumscribed opportunities where the voting equipment must be serviceable for the voters; it must function to record and process votes accurately during the limited time any voter is present or those votes may be lost and those voters disenfranchised.

TTBR and EVEREST produced three overall conclusions highly germane to whether fundamental voting rights are achieved. First, the operations of these voting systems are controlled by software so significantly flawed that those who teach software design and coding have pronounced it *unfit for high confidence in its accuracy and reliability.*[79] Second, they conclude that the software—the controls

ballots cast and the number of votes counted).

[78] *Id.* at 2.

[79] As TTBR co-principal investigator Matt Bishop summarized, "The red 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." BISHOP, *supra* note 64, at 11; *see also* EVEREST EXECUTIVE REPORT, *supra* note 54, at

over the entire election processes culminating in a cast votes report—*is unable to provide assured accountability for whether the product has functioned normally—accurately—in election operations***.**[80]

Thus, in 2007, an array of the most widely respected experts in computer science and voting systems software informed us that the equipment that determines whether fundamental rights to vote will be fulfilled offers vast reasons not to trust the election outcomes this equipment produces. Further, breaching the basic precepts of information systems design where data accuracy and security are crucial objectives, the equipment does not provide trustworthy electronic self-reporting on core performance, including whether the equipment has operated as intended in allocating votes to candidates or counting ballots from all precincts.[81] Those with vast knowledge of both the software industry's engineering standards and the tools for diagnosing anomalies have counseled the public and election officials that without other corrections and quality assurance steps,[82] these machines are unfit for voting.

If engineering assessments of a commercial aircraft were equally negative regarding the aviation software's compliance with the industry's best practices for assuring human safety, the Federal Aviation Administration has the power and the staff expertise to declare it "not airworthy."[83] Such aircraft must remain grounded until

14–72 (EVEREST private consultants concluding that all of the voting systems fell well below reasonable engineering expectations, with Diebold/Premier & Hart scoring zero of twelve possible points and ES&S scoring one point). *See also supra* text accompanying notes 57–65.

[80] Private sector IT security firm MicroSolved "concluded that the voting machine companies have failed to adopt, implement and follow industry standard best practices in the development of the system." EVEREST EXECUTIVE REPORT, *supra* note 54, at 15 (internal quotation marks omitted). These conclusions may be analogized to expert civil engineers reporting that a major transportation bridge was not engineered consistent with industry standards, and is unfit for carrying traffic.

[81] Rather stunningly, voting systems logging functions that monitor performance have not been designed to be automatic and impervious to change. Unlike aircraft flight recorders and financial institution accounting software, those who are "insiders" and considered to have a conflict of interest are able to manually configure voting systems' logs, the purpose of which are to report on system and operator performance. *See, e.g.*, UC SOURCE CODE REVIEW, *supra* note 35, at 36 (identifying "Issue 5.1.4: The audit log does not adequately detect malicious tampering"); *id.* at 53 (noting "Issue 5.3.2: Anyone with access to the GEMS server's local disk can modify the GEMS database," which includes the audit logs).

[82] *See infra* note 156 and accompanying text (discussing how voting equipment that is controlled by flawed software can still be used to achieve accurate election results).

[83] "An airworthy aircraft is one that is fit to fly." *Airworthiness*, SKYBRARY, http://www.skybrary.aero/index.php/Airworthiness (last updated Sept. 1, 2011).

Congress has not delegated a power equivalent to the FAA's to ensure voting systems' constitutional or statutory sufficiency. HAVA delegates to the U.S. Attorney General the power to enforce HAVA's minimum standards for voting equipment accuracy, auditability, accessibility and other requirements. Other than enforcing alternative language and accessibility requirements, the Department of Justice has basically ignored its HAVA enforcement duties modifications and further assessments declare it airworthy. In contrast, although both voting and aviation require quality engineering to achieve accuracy in operations, no federal agency is empowered to issue analogous judgments and orders regarding the engineering inadequacy of voting systems. Further, under the regulatory rules governing flight performance data recorders in commercial aircraft, by design and operation the data recorders are protected from the aircraft carrier's control, from the pilot's influence, and even from horrific crash disasters.[84] The information systems industry has engineered data recording systems worthy of trust even in extremely challenging physical conditions, such as those of aviation disasters, and could do so for voting systems but the qualified TTBR and EVEREST assessors reported that the voting industry did not implement auditing designs that warrant trust in the equipment's output.

The third core conclusion the scientific studies reached is equally critical for voting rights: *all of the deployed e-voting systems have incorporated multiple, easily utilized pathways for motivated insiders to subvert elections without a trace*.[85] 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."[86] Translated into traditional considerations for election law, the deployed e-voting systems have allowed numerous secret methods for dishonest or highly partisan vendors, vendor personnel (including software programmers), election office staff, poll workers or voters to engage in the electronic equivalent of ballot box stuffing[87] and to erase any tracks back to

under Title III.

[84] *See Flight Data Recorders (FDR)*, SKYBRARY, http://www.skybrary.aero/index.php/Flight_Data_Recorder_(FDR)#Principles_of_Operation (last updated June 16, 2011) ("The recorder is installed in the most crash survivable part of the aircraft, usually the tail section. The data collected in the FDR system can help investigators determine whether an accident was caused by pilot error, by an external event (such as windshear), or by an airplane system problem."). Though election logging functions do not need to withstand a crash from 50,000 feet, they should be engineered for realistic election conditions; some minimum standards are specified in the federal Voluntary Voting System Guidelines. *See* 1 UNITED STATES ELECTION ASSISTANCE COMM'N, VOLUNTARY VOTING SYSTEM GUIDELINES § 2.1.5.1 (2005) (listing minimum requirements that voting systems should meet and stating that "[a]udit records shall be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors").

[85] *See* EVEREST EXECUTIVE REPORT, *supra* note 54, at 15 ("[T]here was a lack of integrity controls that have been applied to the voting systems . . . . [There are] vulnerabilities in all three voting systems that could allow attackers to introduce an infection or malicious programming (malware) into the voting system.") (internal quotation marks omitted).

[86] *Id.* at 35.

[87] In Gray v. Sanders, 372 U.S. 368, 380 (1963), the Court stressed that the right to vote

themselves. Some vendors even included design elements that practically invite tampering, such as including a "clear" button for erasing audit logging of operator actions inside the tabulation database.[88] This option permits someone to modify vote totals for a race, such as by flipping the results between candidates, and then erasing the automatic record that would have recorded the data modification.[89] The bottom line security point: use of all-electronic voting equipment without quality assurance techniques that rely on a tangible record of the voter's choices independent of the electronic equipment permits nefarious conduct to convert voting rights into an illusion.[90]

In legal challenges to all-electronic voting systems, the judiciary has thus far failed to address the TTBR and EVEREST conclusions that the scientific community considers to be definitive studies. Recent judicial rulings continue to rely on precedent that preceded the TTBR and EVEREST reports.[91]

---

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,* 238 U.S. 383, 386 [(1915)], "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. *Ex parte Siebold*, 100 U.S. 371 [(1879)]; *United States v. Saylor,* 322 U.S. 385 [(1944)].

see also Reynolds v. Sims, 377 U.S. 533, 554–55 (1964) ("Undeniably the Constitution of the United States protects the right of all qualified citizens to vote . . . . The right to vote can neither be denied outright, nor destroyed by alteration of ballots, nor diluted by ballot-box stuffing.") (citations omitted); Baker v. Carr, 369 U.S. 186, 208 (1962) ("A citizen's right to a vote free of arbitrary impairment by state action has been judicially recognized as a right secured by the Constitution, when such impairment resulted from dilution by a false tally, or by a refusal to count votes from arbitrarily selected precincts, or by a stuffing of the ballot box.") (internal citations omitted); 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 at Congressional elections.").

[88] *See* DEBRA BOWEN, CALIFORNIA SEC'Y OF STATE, REPORT TO THE ELECTION ASSISTANCE COMMISSION CONCERNING ERRORS AND DEFICIENCIES IN DIEBOLD/PREMIER GEMS VERSION 1.18.19, 7 (2009) ("GEMS version 1.18.19 is designed to permit the operator to delete the audit trail records in two important audit logs, intentionally or inadvertently. The records can be deleted by selecting 'Clear' buttons that appear on the audit log screens between the 'Save As…' and 'Close' buttons.").

[89] *Id.*

[90] In other words, the conclusion that the software is seriously flawed and should not be trusted does not necessarily require that the voting systems be discarded. Certain procedural steps permit the identification and correction of errors. *See* P.B. Stark & D.A. Wagner, *supra* note 63 (arguing "that there should be more focus on regulating procedures, especially the curation of the audit trail, and less focus on certifying tabulation equipment, in part because *certification can never guarantee that votes are tabulated accurately in practice*") (emphasis added).

[91] *See, e.g.*, Andrade v. NAACP of Austin, 345 S.W.3d 1 (Tex. 2011) (ruling that the Texas Secretary of State had the power to balance relative assets and deficiencies of the

D. Emerging Threats

The need for judicial attention to the problems of e-voting is becoming more pronounced, as vendors are now aggressively marketing voting systems to state and local governments with even more security holes than the currently deployed precinct-based voting systems. Vendors are currently pressing state governments to permit Internet transmission of voted ballots on their proprietary software.[92] Over half the states have now approved Internet voting for military and overseas civilian voters[93] despite the computer security community's virtual unanimity regarding the grave dangers this poses to individual ballots and systemic integrity. The scientists have underscored that Internet-transmitted ballots will eliminate the capacity to assure that the ballots of only authorized voters will be counted, and that ballots will arrive with the same vote choices the voter originally marked.[94] Additionally, such all-electronic Internet systems provide no external audit capacity,[95] so whatever totals the election officials announce cannot be recounted or otherwise checked; the results could be completely falsified by foreign adversaries or be a product of software bugs yet would provide no extrinsic evidence as a

challenged all-electronic DRE voting systems, and that under a rational basis review, the court lacked the power to displace that judgment).

[92] For instance, the state legislatures in Connecticut, Colorado and Oregon have considered bills that would authorize Internet voting for domestic voters and not simply military and overseas civilian voters.

[93] Verified Voting's informational webpage identifies thirty–three States that authorize electronic voting ballots to be returned via an Internet–based (web portal, e–mail, or fax) method for military personnel and citizens overseas. *Internet Voting Information: Military and Overseas Voting 2012*, VERIFIED VOTING FOUNDATION, http://www.verifiedvotingfoundation.org/article.php?list=type&type=27 (last visited May 10, , 2012). An obscure Federal agency within the personnel division of the Department of Defense has lobbied state governments to adopt Internet voting for military and overseas civilian voters. *See generally* Candice Hoke & Matt Bishop, Essential Research Needed to Support UOCAVA-MOVE Act Implementation at the State and Local Levels (Oct. 25, 2010) (unpublished manuscript), *available at* http://dx.doi.org/10.2139/ssrn.1697848.

[94] For example, MIT computer scientist and cryptography expert Professor Ron Rivest opposes Internet voting because we do not yet have the necessary technology to implement secure online voting systems. *See* 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 ("'We don't have the technology yet to do this in a secure way, and we may not for a decade or more,' says Ron Rivest, a computer scientist and cryptography expert at MIT. The worst-case scenario? 'You may find elections that end up with a totally unclear result,' Rivest says. 'You may find the entire system taken over and trashed.'").

[95] *See, e.g.*, David Jefferson*, If I Can Shop and Bank Online, Why Can't I Vote Online?* 3 (2011), http://electionlawblog.org/wp-content/uploads/jefferson-onlinevoting.pdf ("[I]n the online election world there are no receipts, no double entry bookkeeping, and no meaningful audit trail information.").

check.[96] Information security experts emphasize that the Internet was not engineered for secure data transmissions,[97] and, without that security, voted ballots cannot be trusted to arrive in the same version as the remote absentee voter intended.[98]

Given that U.S. elections are considered high value, easy targets for cyber attack,[99] and that virtually every major U.S. government and private sector defense industry network has been breached with a sophisticated cyber attack despite their defensive apparatus,[100] the cyber security experts conclude that no reasonable basis exists for trusting that an Internet-based election will not be falsified in some manner.[101] They caution that even if ballots are encrypted, hundreds of vectors remain available for impacting the integrity of an Internet

[96] *See generally* P.B. Stark & D.A. Wagner, *supra* note 63 (explaining the tools that can produce evidence of accuracy and inaccuracy in election tallies, and obviate the mystifying "black box" of e-voting).

[97] *See generally* MATT BISHOP, COMPUTER SECURITY: ART & SCIENCE (2002) (clarifying that public networks are pervaded with dangerous threats that include such malware as viruses, worms, botnets; complete defenses remain unavailable); Jonathan Zittrain, *Without a Net: The Internet Is Vulnerable to Viruses so Lethal That They Could Gravely Damage the Online World–Unless We Upgrade Law and Technology Now*, LEGAL AFFAIRS (Jan.–Feb. 2006), http://www.legalaffairs.org/issues/January-February-2006/feature_zittrain_janfeb06.msp ("[A]lthough hundreds of millions of personal computers are now connected to the Internet and ostensibly protected by firewalls and antivirus software, our technological infrastructure is in fact less secure than it was in 1988.").

[98] *See In Theory And Practice, Why Internet–Based Voting Is a Bad Idea*, SLASHDOT (Mar. 2, 2012, 4:47 PM), http://politics.slashdot.org/story/12/03/02/1940236/in-theory-and-practice-why-Internet-based-voting-is-a-bad-idea [hereinafter *Bad Idea*] (arguing that Internet voting systems can be easily manipulated "because the structure of an electronic voting system is inherently complex . . . it's difficult if not impossible to roll back results if a compromise is suspected[,] . . . [and,] [u]nlike paper ballots[,] . . . online vote gathering offers no good way to re-count").

[99] *See, e.g.*, Professor Ronald Rivest, Power Point Presentation: Thoughts on UOCAVA Voting (Aug. 6, 2010), http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/RIVEST_2010-08-05-uocava.pdf (concluding that the likelihood of a successful attack on a U.S. Internet-conducted election is 100 percent); David Jefferson, Power Point Presentation: Internet Voting for UOCAVA Voters (Aug. 6, 2010), http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/JEFFERSON_UOCAVA_Workshop_Panel.pdf (emphasizing that election integrity is a national security matter).

[100] Formerly Director of National Intelligence and now a private security consultant, Mike McConnell commented, "In looking at computer systems of consequence—in government, Congress, at the Department of Defense, aerospace, companies with valuable trade secrets—*we've not examined one yet that has not been infected by an advanced persistent threat.*" Nicole Perlroth, *Traveling Light in a Time of Digital Thievery*, N.Y. TIMES, Feb. 10, 2012, at A1 (emphasis added). An Advanced Persistent Threat (APT) is considered the most serious and persistent type of cyber-attack, designed by "a sophisticated and organized" attacker to "access and steal information from compromised computers . . . intruders responsible for the APT attacks target the defense industrial base (DIB) [and the financial, manufacturing, and research industries]. The attacks used by the APT intruders are not very different from any other intruder. The main differentiator is the APT intruder's perseverance and resources." *Advanced Persistent Threat*, MANDIANT, www.mandiant.com/services/advanced_persistent_threat (last visited May 10, 2012).

[101] *See* David Jefferson, *The Dangers of Email Voting,* (2011) (draft on file with author).

election.[102] Though online ballot marking systems and complete Internet voting that transmit blank and marked ballots through the Internet unquestionably cannot offer confidence that they will be received without en route falsification thus to be counted as cast,[103] states are adopting these systems. Unfortunately, thus far no state or local official or their vendors are disclosing these vulnerabilities to voters.[104] Nor do legislators and election officials generally comprehend the national security aspects of elections vulnerable to covert cyber attacks from abroad.[105] Apparently election officers and

[102] *See, e.g.*, Jefferson*, supra* note 95, at 2–3 ("We have to recognize that the cost to the attacker of conducting a remote online attack has declined drastically over the last few years . . . . [I]t [is] possible to duplicate even very sophisticated attack vectors like Stuxnet, the malware that did great damage to Iranian nuclear facilities, in about two months time for under $20,000. We are now in a very different threat environment than we were even a few years ago.") (citation omitted); Jaikumar Vijayan, *Internet Voting Systems Too Insecure, Researcher Warns*, COMPUTERWORLD (Mar. 1, 2012, 12:13 PM) http://www.computerworld.com/s/article/9224799/Internet_voting_systems_too_insecure_researcher_warns?taxonomyId=17&pageNumber=2 ("[A] team of researchers [was able to] easily [break] into [Washington state's electronic voting] system, and show[] how they could modify and replace marked ballots in the system. The researchers even tweaked the system so that voters would be greeted with the University of Michigan fight song when they landed on the vote confirmation page."); *see also* Jeremy Epstein, *Internet Voting, Security, and Privacy,* 19 WM & MARY BILL RTS. J. 885 (2011) (explaining the technical problems of Internet voting systems and their dangerous impact for voting rights and election integrity); Barbara Simons & Doug W. Jones, *Internet Voting in the U.S.*, ACM Library (2011) (same). *But see* MICHAEL ALVAREZ & THAD HALL, POINT, CLICK AND VOTE: THE FUTURE OF INTERNET VOTING 4–11 (2004) (perceiving great promise and manageable security threats in Internet voting and contending that "a strong argument can be made for pilot testing Internet voting systems in real elections").

[103] During the public test of the District of Columbia's Internet voting system, Professor Halderman was able to attack the system and "replace all of the encrypted ballot files on the server . . . with a forged ballot of [his] choosing." Scott Wolchok et al., *Attacking the Washington, D.C. Internet Voting System* 7 (2012), http://fc12.ifca.ai/pre-proceedings/paper_79.pdf.; *see also* David Jefferson & Candice Hoke, *The Dangers of On-Screen and Online Electronic Ballot Marking* (2012) (draft on file with author).

[104] States adopting these online ballot marking systems include Colorado, *see Electronic Voting Systems Fact Sheet*, FEDERAL VOTING ASSISTANCE PROGRAM, http://www.fvap.gov/resources/media/evswfactsheet.pdf (last visited Apr. 15. 2012) ("[Six] Colorado counties (El Paso, Gilpen, Morgan, Park, Weld, and Yuma Counties) offer a state system which allows voters to mark the ballot online."), and Maryland, *see* S. 1078, 2012 Gen. Assemb. 430th Sess. (Md. 2012) ("The State Board of Elections (SBE) must provide an optional online ballot marking tool . . . ."). *But see* Letter from Debra Bowen, Cal. Sec. of State, to all County Clerks/Registrars of Voters (Nov. 8, 2011), *available at* http://www.sos.ca.gov/elections/ccrov/pdf/2011/november/11111lf.pdf ("[Voting systems with] an option to mark votes on the ballot using the voter's computer . . . [are] not permitted for use in California under state law.").

[105] *See* Jefferson, supra note 95, at 1, 3 ("[C]omputer and network security experts are virtually unanimous in pointing out that online voting is an exceedingly dangerous threat to the integrity of U.S. elections. There is no way to guarantee that the security, privacy, and transparency requirements for elections can all be met with any practical technology in the foreseeable future. . . . Election security is . . . a matter of *national security* . . . ."); *Bad Idea, supra* note 98 ("The risk of hacked elections isn't just the possibility of political rivals trying to out-do each other[.] . . . [U]ltimately, vulnerable election systems compromise national security and ballot secrecy.").

their lawyers have yet to translate the TTBR and EVEREST conclusions concerning these all-electronic voting systems into the concepts and categories relevant to election law, such as unlawful "vote dilution"[106] or failures to produce provably accurate elections.

II. "LENSES" AND LEGAL FRAMEWORKS

Professor Richard Hasen has identified constitutional law and political science as the progenitors of election law in light of these fields' profuse scholarship on voting rights, campaign finance, and redistricting.[107] In order for scientific facts about currently deployed voting systems to guide voting technology policy and adjudication,[108] perhaps the time has come for election law scholars to enlarge the recognized "parents" of election law. Given the centrality of voting technology adequacy to realizing the fullness of voting rights and popular sovereignty, it appears overdue for election law to embrace the computer science and information security fields[109] as a co-equal nurturing "parent"—or at least as a valued aunt or uncle—of election law.

Political science categories and research methodologies have supplied crucial information and valuable heuristics relevant to the legal sufficiency of certain types of voting technologies. For instance, by questioning "residual vote rates"[110] researchers were able to study the relationship between lost votes and voting technologies, and to establish that voters of racial and ethnic minority groups generally

[106] *See* Heather K. Gerken, *Understanding the Right to an Undiluted Vote*, 114 HARV. L. REV. 1663, 1665 (2001) (arguing that vote dilution claims relate to aggregative rights of groups which cannot be adjudicated within the conventional individual rights framework).

[107] *See* Richard L. Hasen, *Election Law at Puberty: Optimism and Words of Caution,* 32 Loy. L.A. L. Rev. 1095, 1095 (1999) (naming constitutional law and political science as the "parents" of election law).

[108] My objective accords with Heather Gerken's as she calls for "hard data and rigorous analysis" to drive election policy. Some of the hard data and analytic frameworks missing thus far must be found in information security rather than political science. *See* HEATHER GERKEN, THE DEMOCRACY INDEX: WHY OUR ELECTION SYSTEM IS FAILING AND HOW TO FIX IT 5859 (2009) (drawing on Dan Tokaji's "moneyball" approach).

[109] Federal policymakers have recently decided that they would like to combine the different terms for information system security into one term, cybersecurity, which embraces the entire field from individual computing devices to networks as large as the Internet. "*Shaping the Future of Cybersecurity Education" Workshop*, NIST (Sept. 20–22, 2011), http://csrc.nist.gov/nice/Sept2011-workshop/.

[110] Political scientists crafted the term and its empirical assessments in part to determine whether racial and ethnic minorities voting power had been diminished disproportionately because of voting technology. *See, e.g.*, The Caltech/MIT Voting Technology Project, *Residual Votes Attributable to Technology: An Assessment of the Reliability of Existing Voting Equipment* 1–2 (Mar. 30, 2001), http://vote.caltech.edu/drupal/files/report/residual_votes_attributable_to_tech.pdf (examining incidence of spoiled and unmarked ballots, termed the residual vote rate, associated with each type of voting equipment).

were allocated equipment that permitted substantially higher error rates.[111] Litigation could then successfully challenge particular voting technologies as legally insufficient for underserved minorities' full voting participation.[112]

Political science, however, has not supplied sufficient analytic frameworks and methodologies by which other legally relevant deficiencies in voting technology can be identified. As demonstrated above,[113] the computer or information security subfield of computer science supplies powerful tools—better lenses as it were—for perceiving and understanding serious technological flaws that relate to voting rights; these flaws remain largely invisible if using only political science methods or "lenses."

It may be that information system and security concerns have fallen prey to the supposed dichotomy and debate in election law between assuring voter "access" or ensuring the "integrity" of the vote count.[114] Since one's position on the access/integrity divide has often been viewed as code for political party commitment, and the "integrity" side has accumulated a multi-year sordid record for attempted voter suppression on the basis of spurious claims of voter fraud,[115] the wrongful classification of computer security points as

[111] *Id.*

[112] Litigation where structural challenges to voting technology were predicated on the Equal Protection Clause, the Due Process Clause and section 2 of the Voting Rights Act include *Stewart v. Blackwell*, 444 F.3d 843 (6th Cir. 2006), *vacated as moot* 473 F.3d 692 (2007), and *Black v. McGuffage*, 209 F. Supp. 2d 889 (N.D. Ill 2002).

[113] See supra Part I.

[114] The conception persists that access and integrity are opposed values that also function as thin shields for partisan opportunism. *See, e.g.*, Richard L. Hasen, *Beyond the Margin of Litigation: Reforming U.S. Election Administration to Avoid Electoral Meltdown*, 62 WASH. & LEE L. REV. 937, 983–85 (2005) (advocating a model of nonpartisan election administration with an allegiance to the "integrity of the process itself," rather than "to any particular electoral outcome"); Daniel P. Tokaji, *Early Returns on Election Reform: Discretion, Disenfranchisement, and the Help America Vote Act,* 73 GEO. WASH. L. REV. 1206, 1233 (2005) (describing "HAVA's access/integrity compromise"); *see also* Christopher S. Elmendorf, *Refining The Democracy Canon,* 95 CORNELL L. REV. 1051, 1058 (2010) (responding to Rick Hasen's conception of the Canon as detailed in Richard L. Hasen, *The Democracy Canon,* 62 STAN. L. REV. 69 (2009)). As these scholars have clarified, "access" constellations of issues have been conceptualized as concerned with expanding voter participation and removing barriers to voting. *Id.* at 1051. As such, some consider these core Democratic Party concerns, and further view a genuine commitment to voter access and broad civic participation to justify "convenience . . . voting." Daniel P. Tokaji & Ruth Coker*, Absentee Voting by People with Disabilities: Promoting Access and Integrity*, 38 MCGEORGE L. REV. 1015, 1027 (2007). At the other supposed pole, "integrity" values have sometimes been used to justify tremendous burdens on voter participation, such as by arduous voter identification requirements, as have thus been viewed Republican Party's domain. *Id.* at 1043. This author joins others who view the access/integrity split as a false dichotomy. *Id.*

[115] *See* RICHARD HASEN, THE VOTING WARS (forthcoming 2012) (detailing thinly veiled voter suppression efforts conducted under the flag of achieving integrity"); WENDY R. WEISER AND LAWRENCE NORDEN, VOTING LAW CHANGES IN 2012 33 (2011) (discussing Ohio voter-suppression legislation).

exclusively "integrity" concerns may have led to their receiving little traction among election law scholars.[116]

By shifting to a different field of expertise, though, the change in central concerns and methodologies can in turn bring forward powerful new perceptions. Using computer or information security "lenses," the central triadic planes for analysis become system "availability" for use as intended,[117] confidentiality, and data "integrity"—the last of which captures "both the correctness and the trustworthiness of the data."[118] Computer security is therefore deeply concerned with the voting equipment's availability and reliability for casting ballots, and hence to traditional "access" concerns.

Classifying the voting system computer security assessments as relating only to "integrity" is thus wrong in two ways. It excludes the field's core concerns for achieving effective use of the technical equipment, embracing reliability and voter access. Additionally, when a claim is made that the security studies only relate to "integrity," grave miscommunication occurs because the field's conception of "integrity" differs in depth and centrality that neither election law nor political science has yet grasped.

Properly characterized in terms that the Fourteenth Amendment comprehends, for instance by using voting participation or access rights, vote dilution, and ballot box stuffing, the particular threats presented by all-electronic, unverifiable voting systems can be effectively redressed by the judiciary. The initial challenges have focused on all-electronic DRE systems, but all e-voting systems are capable of flawed tabulations; fortunately, however, these errors normally can be caught and corrected by use of robust post-election auditing techniques.[119]

A. Litigation Challenging DREs

Three federal circuits[120] and state courts in Arizona,[121] Texas,[122] Pennsylvania,[123] Maryland,[124] Georgia,[125] and New Jersey[126] have

[116] Additionally, because the debate has also been framed as a set of ineluctable tradeoffs between civil rights objectives and their political opponents, the information security experts' concerns may have been tacitly rejected under the assumption that accessibility or voter convenience would inevitably be diminished taking into account information security concerns.

[117] *See* MATT BISHOP, INTRODUCTION TO COMPUTER SECURITY 1, 4 (2003) ("Computer security rests on confidentiality, integrity, and availability.").

[118] *Id.* at 3.

[119] *See infra* text accompanying note 157.

[120] Weber v. Shelley, 347 F.3d 1101, 1103 (9th Cir. 2003) (holding that all-electronic DREs lacking a voter-verified paper record do not deprive voters of legal rights); Wexler v. Anderson, 452 F.3d 1226, 1233 (11th Cir. 2006) (same); Tex. Democratic Party v. Williams, 285 F. App'x. 194, 195 (5th Cir. 2008) (per curiam), *cert. denied,* 129 S. Ct. 912 (2009) (affirming summary judgment in favor of Secretary of State on claims that DRE deprived voters

ruled on claims that electronic DRE-touchscreen voting devices are constitutionally invalid if they lack a voter-verified contemporaneous paper record of the vote selections. Thus far, the courts have not been particularly receptive to these claims, whether predicated on the Fourteenth Amendment[127] or the state constitutions.

Irrespective of how the claims were legally grounded, the courts that ruled against the plaintiffs chose a deferential standard of review that largely insulated the pre-existing policy decision. *Schade v. Maryland*, for instance,[128] is somewhat of an exemplar. There the court applied an extremely deferential "arbitrary and capricious" standard of review that the State Board of Elections urged, resulting in no relief for the plaintiffs. Although the state legislature had retained a highly experienced cyber security expert to conduct a security analysis of the proposed DRE system,[129] the Maryland courts did not accord his team's assessment and recommendations with authoritative weight. Instead, the court found the Board's computer science expert—who also was an attorney—a more credible expert, perhaps because he knew how to translate between the two fields. Although this expert lacked professional credentials as a computer security expert, the trial court qualified him as such nonetheless and permitted him unlimited expert scope. He then testified to the "reasonableness" of the Board's choice of paperless DREs that lacked any record independent of the problematic software. He also testified

of equal protection and due process and violated the Election Code).

[121] Chavez v. Brewer, 214 P.3d 397, 408–09 (Ariz. Ct. App. 2009) (ruling that plaintiffs' claims survived a motion to dismiss, specifically that voting machines violated the Arizona Constitution's "free and equal election" clause and the "privileges and immunities" clauses).

[122] Andrade v. NAACP of Austin, 345 S.W.3d 1, 14 (Tex. 2011) (ruling that the Texas Secretary of State had the power to balance relative assets and deficiencies of the challenged all-electronic DRE voting systems, and that under a rational basis review, the court lacked the power to displace that judgment).

[123] Banfield v. Corte*s*, 922 A.2d 36, 42 (Pa. Commw. Ct. 2007) (refusing to dismiss electors' claims that secretary of state had illegally certified DREs).

[124] Schade v. Md. State Bd. of Elections*,* 930 A.2d 304, 328 (Md. 2007) (deferring to the state board of elections's judgment in certifying DREs that lacked a voter verified paper audit trail).

[125] Favorito v. Handel*,* 684 S.E.2d 257, 261–62 (Ga. 2009) (deferring to a political branch).

[126] Gusciora v. Corzine, No. MER–L–2691–04, 2010 N.J. Super. LEXIS 2319, 2332–33 (N.J. Super. Ct. Law Div. 2010) (holding that State's certification of DREs did not violate voters' equal protection or due process rights but mandating mitigations that the plaintiffs' premier security experts had demonstrated to be ineffectual).

[127] The federal constitutional claims under the Fourteenth Amendment have been predicated on the Equal Protection Clause or substantive or procedural due process. U.S. CONST. amend. XIV.

[128] 930 A.2d at 326.

[129] RABA study, *supra* note 26.

to the historic security issues with paper ballots, explicitly opining that the introduction of an auditable permanent record of the voter's choices extrinsic to the voting machine would increase the security problems rather than cure them.[130] Yet this expert had testified to the Texas legislature with quite different concerns and conclusions, completely in line with those of the TTBR and EVEREST scientists largely contradicting his Maryland testimony.[131]

The most recent DRE decision, from the Texas Supreme Court in 2011, was predicated on state statutory and constitutional law. The NAACP of Austin and individual plaintiffs claimed that the Secretary of State's "failure to require a contemporaneous paper record of an electronic vote violates their statutory right to a recount and an audit, as well as Texas constitutional guarantees of equal protection, the purity of the ballot box, and the right of suffrage."[132] While the Court granted plaintiffs standing on their equal protection claims, it chose a deferential "sliding scale" standard of review drawn from other election administrative cases. After quickly reviewing the line of prior

[130] Additionally, the court credited the National Federal for the Blind's arguments that a paper ballot would destroy their members' opportunities to vote "privately" and "independently." Schade v. Md. State Bd. of Elections*,* 930 A.2d 304, 312 (Md. 2007).

[131] *See* Roy G. Saltman, U.S. Dep't. Of Commerce, *NBS Special Publication 500–158, Accuracy, Integrity, And Security In Computerized Vote–Tallying* 1, 18–20 (1988), http://www.itl.nist.gov/lab/specpubs/500-158.htm:

> [T]he computer hardware and software used to tabulate the ballots is subject to tampering. Furthermore, such tampering is relatively easy and invisible.... Computers can be manipulated remotely, by wire or radio, or by direct physical input. The memories on which these computers operate can easily fit into a shirt pocket and can be substituted in seconds. The software can be set to await the receipt of a special card, whose presence will cause all the election counters to be altered. This card could be dropped into the ballot box by any confederate. *The possibilities for this type of tampering are endless, and virtually no detection is possible once tabulation has been completed* . . . .
>
> *Even if the software is not altered, there is no reason to believe that it is correct.* Many tests performed on such programs have *revealed faulty logic and wildly incorrect results* . . . . Many jurisdictions, such as Pennsylvania, have complex rules for counting such situations as cross-filed candidates in vote-for-many offices and *it is stretching to believe that an election system vendor would be aware of all such combinations of conditions to have produced perfect software.* It is *axiomatic in the computer industry that all large computer programs contain errors, and the more extensive the software the more errors it contains....*
>
> *When one company or a conglomerate of companies supply unauditable software from a central distribution point, or participate directly in ballot setup procedures, there exists the possibility of large-scale tampering with elections. An errant programmer or tainted executive could influence or determine the outcome of a majority of election precincts in the country* . . . .

(quoting Dr. Michael I. Shamos's testimony before the Texas legislature) (emphasis added).

[132] Andrade v. NAACP of Austin, 345 S.W.3d 1, 6 (Tex. 2011).

DRE decisions, the Texas court followed the same analytic approach that was first used in *Weber v. Shelley*,[133] a case decided in 2003 that preceded all of the scientific assessments of voting systems. As in *Weber*, the Texas court viewed DREs to offer some significant advantages for certain classes of voters though also presenting some drawbacks.[134]

The court followed Professor Dan Tokaji's approach of perceiving the interest of all voters in an undiluted ballot to be of mere hypothetical concern, whereas the supposed DRE accessibility features for physically disabled voters were concrete improvements for underserved populations. To the degree these two sets of concerns were perceived to be in tension,[135] Tokaji and the Texas court considered the accommodation objective of superior importance.[136] Using highly deferential legal scrutiny, the court concluded that it must defer the choice of voting technologies to the regulatory decisions of the Texas Secretary of State.

The court's perception of opposed objectives that justifies deference rested on a superficial understanding of computer security and misconceived the court's role in achieving accessibility. The

[133] 347 F.3d 1101, 1106–07.

[134] "DREs are not perfect. No voting system is. We cannot say that DREs impose severe restrictions on voters, particularly in light of the significant benefits such machines offer." *Andrade,* 345 S.W.3d at 14. The major difference between *Andrade* and the earlier decisions lies in the Texas court's reliance on Daniel Tokaji's elaboration of four "equality norms" in federal voting rights law. Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1741 (2005). He draws the four norms from anti-discrimination law, particularly the Voting Rights Act and Americans with Disabilities Act of 1990, to yield racial equality, disability access, multi-language access, and inter–jurisdictional equality. *Id.* at 1741–54. By contrast, Heather Gerken recognizes that the right to be free from vote dilution, to have one's ballot counted as cast and reflected in the tally, has not been limited to classic antidiscrimination contexts. *See* Gerken, *supra* note 106 (stressing freedom from vote dilution is an essential part of the structural, "aggregative" concept of voting rights, which are held co-equally by all voters).

[135] *See Andrade*, 345 S.W.3d at n. 22 quoting one commentator who suggests that requiring contemporaneous paper records of DRE votes is problematic:

> First, it relies on the false assumption that paper-based systems are inherently more accurate and reliable than paperless ones. Second, it disregards both long and recent experience demonstrating the vulnerability of paper-based systems to fraud and error. Third, it fails to comprehend the practical problems in actually implementing a system that is capable of printing out a contemporaneous paper record, yet preserves voter privacy and election security.

(quoting Tokaji, *supra* note 134, at 1780–81); *see also id.* at 1736 (noting that "many election officials and some civil rights advocates have opposed a contemporaneous paper record requirement, arguing that it is unnecessary, burdensome, and likely to discourage adoption of accessible voting technology").

[136] *Id.* at 1795. Arguably, this approach reflects misunderstandings of the relation of computer security design and robust coding function in the overall fulfillment of the right to vote on computer-based equipment.

court, moreover, lacked an understanding of how computer security functions in the overall fulfillment of voter access and the right to vote on computer-based equipment. The computer security field is partly predicated on the insight that the electronic equipment's performance—its very availability and capacity to function for the target audience, whether accessible voting systems or any others—is substantially dependent upon the constellation of attributes that the computer science field sums as its "security." Thus, security is not at war with accessibility but, joined by usability, provides the very foundation on which accessibility features rest. A grossly insecure system, be it paperless DREs or any other, is likely to be an accessible voting device in theory only.[137] Field testing and security attributes matter to whether accessible voting equipment requirements have been achieved for real voters.

In contrast, rulings from the Sixth Circuit arguably present a more defensible decisional framework. While the Sixth Circuit has not ruled on a case seeking to invalidate DREs, it has issued opinions in a triad of cases presenting equal protection and substantive due process challenges to Ohio's voting technology choices,[138] its overall election administrative system,[139] and, most recently, one county's application of rules governing the invalidation of provisional ballots.[140] Each opinion displays a keen understanding of the federal judiciary's crucial role in ensuring that state political actors do not structure election operations in ways that arguably result in systematic vote dilution or debasement.

Unlike the courts that deferred to state political actors to determine preferred voting technologies,[141] the Sixth Circuit recognizes that a deferential standard of review cannot provide meaningful judicial protection from election rules governing whether a voted ballot will be counted or whether prohibited vote dilution has occurred.[142] The *Stewart* court's analysis of cases from *Yick Wo* to *Bush* results in distinguishing *Burdick*-type issues from claims that particular voters

[137] Downtime or "unavailability" rates of DREs appear nontrivial given some incident reports. *See supra* notes 70–71.

[138] Stewart v. Blackwell, 444 F.3d 843 (6th Cir. 2006), *vacated as moot,* 473 F.3d 692 (2007).

[139] League of Women Voters of Ohio v. Brunner, 548 F.3d 463 (6th Cir. 2008).

[140] Hunter v. Hamilton Cnty. Bd. of Elections, 635 F.3d 219 (6th Cir. 2011).

[141] *See, e.g.*, *supra* note 62, which relied on the *Burdick* precedential line directing rational relation review; *see also* Crawford v. Marion Cnty. Election Bd., 553 U.S. 181 (2008) (further complicating the standard of review questions); Burdick v. Takushi, 504 U.S. 428, 430 (1992) (adjudicating constitutionality of state law omission of a voter option to cast votes for write–in candidates).

[142] *Stewart*, 444 F.3d. at 856.

were denied an equal chance to have their vote counted.[143] Where election rules or ballot counting practices operated at a structural level to threaten the right to an equal voice through the ballot, the Court subjected the challenged practice to strict scrutiny rather than to mere rational relation review.[144]

The Sixth Circuit's argument that the Supreme Court's precedents specify this exacting standard of review is made somewhat more difficult because the Supreme Court has often failed to explicitly specify the standard of review when analyzing an election practice under the equal protection clause.[145] A less careful court might mistake any unnamed analytic method as less than strict scrutiny. But perhaps the best argument for strict scrutiny of structural challenges to a voting technology's constitutional sufficiency can be derived from following the Court's principle of according differential judicial scrutiny to an equal protection claim depending on a threatened right's importance within the constitutional hierarchy.[146]

The Court has consistently placed the right of suffrage at the highest pinnacle of constitutional rights. In *Yick Wo,* the Court characterized the right to vote as a "fundamental political right, because preservative of all rights."[147] Almost a century later, courts observed, "No right is more precious than the right of suffrage. It involves 'matters close to the core of our constitutional system.'"[148] The Court has also stressed, "No right is more precious in a free

[143] *Burdick* is often described as prescribing the standard of review for adjudicating election administrative questions under the equal protection clause. Space constraints prevent depth exploration of *Burdick*'s import for the range of possible voting technology issues potentially presented in litigation; these questions must await later work, Other scholars have addressed *Burdick* and standards of review for election administration more generally. See*, e.g.*, Edward B. Foley, *The Future of* Bush v. Gore, 68 OHIO ST. L.J. 925 (2007); Edward B. Foley, *The Analysis and Mitigation of Electoral Errors: Theory, Practice, Policy*, 18 STAN. L. & POL'Y REV. 350 (2007); *but see* Daniel P. Tokaji, *The Future of Election Reform: From Rules to Institutions*, 28 YALE L. & POL'Y REV. 125 (2009); *see also* Cass R. Sunstein*, The Equal Chance to Have One's Vote Count,* L. & PHIL., 121, 121 (2002).

[144] The Court explicitly applied strict scrutiny in *Dunn v. Blumstein*, 405 U.S. 330, 336–43 (1972) (invalidating Tennessee's residence requirement for voter eligibility), but arguably the ballot box-stuffing cases as well. *See* cases cited *supra* note 87.

[145] *See, e.g.*, Bush v. Gore, 531 U.S. 98 (2000); Harper v. Va. State Bd. of Elections, 383 U.S. 663, 670 (1966) (invalidating poll tax); Gray v. Sanders, 372 U.S. 368 (1962) (invalidating statewide primary election method because it impermissibly accorded votes differential weight depending on demographic features of the voter's location). The Court explicitly applied strict scrutiny in *Dunn v. Blumstein*,405 U.S. 330, 336–43 (1972) (invalidating Tennessee's residence requirement for voter eligibility).

[146] As Rick Hasen remarks, this is "hornbook law." Rick Hasen, Bush v. Gore *and the Future of Equal Protection Law in Elections*, 29 FLA. ST. U. L.REV. 377, 389 (2002).

[147] Yick Wo v. Hopkins, 118 U.S. 356, 370 (1886); *see also* Oregon v. Mitchell, 400 U.S. 112, 139 (1970) (Douglas, J., dissenting and concurring) (observing that the right to vote "a civil right of the highest order").

[148] United States v. Olinger, 759 F.2d 1293, 1302 (7th Cir. 1985) (quoting Carrington v. Rash, 380 U.S. 89, 96 (1965)).

country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined."[149] Given the relative importance of voting rights and the requirement that votes not be diluted or debased, those courts ruling on the legal sufficiency of the DREs must apply strict scrutiny.[150]

B. Scholarly Work Needed

Similarly, given the ample scientific and empirical live-election performance evidence that demonstrates system software can cause vote data to change in an arbitrary and unpredictable manner, and that appropriate steps have not been taken to reduce these risks to voting rights, a substantive due process claim should be available.[151] The Sixth Circuit affirmed that a complaint of errors in DRE vote recording stated a violation of the Due Process Clause if sufficiently unfair as to deny or severely burden Ohioans' fundamental right to vote.[152] It ruled: "[i]f the election process itself reaches the point of patent and fundamental unfairness, a violation of the due process clause may be indicated . . . . Such a situation must go well beyond the ordinary dispute over the counting and marking of ballots."[153] The district court additionally held that the defendant State officers "may be answerable for constitutional violations where state employees have not been trained adequately and that lack of training has caused constitutional wrongs," or if they acted with "deliberate indifference and/or willful blindness."[154]

While these judicial approaches are well designed for protecting the right to vote and popular sovereignty from serious structural dangers posed by misunderstood information technologies, they warrant close evaluation by election law scholars who are considering the concrete systemic threats posed by electronic voting systems. This technological context holds significant but thus far widely unrecognized threats to our system of popular sovereignty. Adjudication under the same standards as whether votes for write-in candidates must be counted, or even whether third parties have ballot access rights to be listed on the ballot, do not compare. One might contend the structural threats the currently deployed e-voting

[149] Wesberry v. Sanders, 376 U.S. 1, 17 (1964).

[150] *See* Hasen, *supra* note 114, at 951.

[151] League of Women Voters of Ohio v. Brunner, 548 F.3d 463 (6th Cir. 2008).

[152] *Id.* at 478.

[153] Griffin v. Burns, 570 F.2d 1065, 1077 (1st Cir. 1978) (citing Brinkerhoff-Faris Co. v. Hill, 281 U.S. 673 (1930)).

[154] League of Women Voters, 432 F. Supp. 2d at 729.

technologies pose to the American electoral system's legitimacy are far greater than any of the prior administrative issues that have been litigated.[155]

To the degree that fiscal concerns are *sub silentio* affecting judicial choice of the standard of review, the judiciary as well as other public officials might be pleased to learn that alternatives to junking the existing machines are available that can solve many of the most egregious issues. The computer security experts with preeminent qualifications in the field have concluded that the best approach is *to not trust the software* to be correct or to produce correct tallies.[156]

[155] Scholars who have addressed the individual vs. structural rights paradigms in voting law include: Vikram D. Amar & Alan Brownstein, *The Hybrid Nature of Political Rights,* 50 STAN. L. REV. 915, 923 (1998) (considering Fifteenth Amendment rights and arguing for a "constitutional model" of voting and other political rights that recognizes both individual and group rights); Heather K. Gerken, *Understanding the Right to an Undiluted Vote*, 114 HARV. L. REV. 1663 (2001); Lani Guinier, *[E]racing Democracy: The Voting Rights Cases*, 108 HARV. L. REV. 109 (1994) (identifying inadequacy of existing voting rights jurisprudence for handling claims involving racial groups); Pamela S. Karlan, *Our Separatism? Voting Rights as an American Nationalities Policy,* 1995 U. CHI. LEGAL F. 83, 84 (arguing voting rights law must reconceptualize "voting-rights remedies to accommodate the claims for representation made by ethnic and racial groups"); *see also* Pamela S. Karlan & Daryl J. Levinson, *Why Voting Is Different,* 84 CAL. L. REV. 1201, 1204–08 (1996) (observing that voting rights law differs from other equal protection contexts as law voters are treated as members of group).

[156] *See, e.g.*, P.B. Stark & D.A. Wagner, *supra* note 63 discussing the requirements of a software-independent system:

> 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 (VVPRs) [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.

Both authors hail from the University of California, Berkeley. Professor David Wagner served as one of the two TTBR leaders and also as the team leader of the Diebold source code team; he also serves on the NIST-EAC Technical Guidelines Development Committee working to develop voting systems standards. Professor Philip Stark, a professor of statistics, served on the post–election audit blue-ribbon panel convened as an ally to the TTBR. Its report, EVALUATION OF AUDIT SAMPLING MODELS AND OPTIONS FOR STRENGTHENING CALIFORNIA'S MANUAL COUNT (2007), assisted the Secretary of State in crafting revised audit standards as a cure for problematic voting systems. *Post-Election Manual Tally Regulations [expired],* CALIFORNIA SECRETARY OF STATE DEBRA BOWEN, http://www.sos.ca.gov/voting-systems/oversight/pemt.htm (last visited May. 10, 2012).

Computer scientists Ron Rivest (of MIT) and John Wack (of the National Institute of Standards and Technology (NIST)), collaboratively originated the concept of "software independence" as part of the NIST-EAC-TGDC effort to develop improved voting systems technical standards. *See* Ronald L. Rivest & John P. Wack, *On The Notion of "Software Independence" In Voting Systems* (draft July 28, 2006),http://rsta.royalsocietypublishing.org/content/366/1881/3759.full.pdf+html (last visited Apr. 15, 2012); *see also* Ronald L. Rivest, *On The Notion Of 'Software Independence' In Voting*

They join others in recommending robust post-election auditing of contemporaneously voter-verified paper ballots as the only feasible way currently available for protecting the election results from tampering and from random miscounts, whether caused by software bugs or other human error. Auditing voter-verified paper ballots can be designed to protect ballot secrecy and yet also provide an effective check on potentially arbitrary or contrived software totals. While the paper ballot record is vulnerable to the classic stratagems that include disappearance, substitution by falsified ballots, or spoilage, a documented chain of custody combined with a random audit conducted by appropriate statistical parameters can supply the needed check and deterrence.[157]

Given that a statistically sound post-election audit of paper ballot voting records can ascertain whether the voting system has counted ballots correctly, and if not, permit a recount, by utilizing this methodology voting rights can be feasibly protected from becoming as insubstantial as electronic pulses. Additionally, because this tool permits humans effectively to "see" inside the machine counts and thus determine whether the count is correct, arguably a substantive due process claim should be actionable where state governments have not adopted auditing processes yet deploy these highly flawed technologies that produce arbitrary vote counts.

When faced with evidence similar to that provided in the TTBR and EVEREST, Germany's Constitutional Court ruled that the electronic vote recording and tabulation systems that were used for electing the Bundestag (national legislature) violated fundamental, systemic protections of democracy and the German citizens' rights to popular sovereignty. The court ruled that the e-voting equipment authorized by the German executive and legislative branches was unconstitutional after evaluating the critical role of public transparency and verification of electoral tallies in assuring democratic legitimacy.[158]

Systems, 366 PHIL. TRANS. R. SOC. A. 3759–3767 (2008) (explaining its use as remedy for errors endemic to computer-based elections systems).

[157] *See id. passim*.

[158] Bundesverfassungsgericht, *Judgment of the Second Senate of 3 March 2009 on the Basis of the Oral Hearing of 28 October 2008* (Mar. 2009), http://www.bverfg.de/entscheidungen/rs20090303_2bvc000307en.html (invalidating the e-voting equipment used in Bundestag elections and holding that public transparency into vote counting processes is constitutionally required). All textual references are drawn from the opinion's paragraphs 109bb–130cc; *see also,* Press Release, Federal Constitutional Court-Press office, *Use of Voting Computers in 2005 Bundestag Election Unconstitutional* (Mar. 3, 2009), http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019en.html; Denise Demirel et al., *Feasibility Analysis of Prêt `a Voter for German Federal Elections* (2011),

> An election procedure in which the voter cannot reliably comprehend whether his or her vote is unfalsifiably recorded and included in the ascertainment of the election result, and how the total votes cast are assigned and counted, excludes central elements of the election procedure from public monitoring, and hence does not comply with the constitutional requirements.[159]

The court rejected as constitutionally insufficient the capacity for expert opinion to pronounce whether the counts were accurate or the software was correct rather than subjected to tampering. The court stressed "the voter himself or herself must be able to verify . . . without a more detailed knowledge of computers."[160]

Additionally, the Constitutional Court held that even when the voter is informed by an electronic display of the fact that his vote has been registered, constitutionally required transparency and verification have not been achieved. It pervasively emphasized the critical role of public transparency and verification to the "democratic legitimacy of the elections," so that "manipulation and unauthorized suspicion can be refuted."[161] The court reasoned, "Only if the electorate can reliably convince itself of the lawfulness of the transfer act . . . before the eyes of the public" can the prerequisites of democratic legitimacy be assured.[162] "Every citizen must be able to understand the key steps of the election without any technical knowledge" so they will respect the announced electoral results. This constitutionally transparency includes the counting of votes.

> An electoral process, in which the voter cannot understand with certainty whether his vote is recorded unaltered, and has been included in the counting of votes, nor how the total votes cast have been accumulated and counted, excludes central components of assured public verification. [It is therefore] unable to satisfy the constitutional requirements.[163]

http://www.ip.ethz.ch/education/techpolicy_series/schedule/Ryan_2a.pdf (pointing out that the court did not invalidate per se e-voting systems but reserved whether any such system could meet public transparency and verification requirements).

[159] Bundesverfassungsgericht, *Judgment of the Second Senate of 3 March 2009 on the Basis of the Oral Hearing of 28 October 2008* ¶ 113 (Mar. 2009), http://www.bverfg.de/entscheidungen/rs20090303_2bvc000307en.html.

[160] *Id.* at ¶ 121.

[161] *Id.* at ¶ 109.

[162] *Id.* (citations and quotation marks omitted).

[163] *Id.*

Thus, Germany's Constitutional Court has realistically faced the challenges of new information technologies to the constitutional rights of its people and its legitimacy as a democratic republic. It has required evidence-based, publicly transparent and verifiable elections rather than permit executive and legislative exhortation that its citizenry should trust in new technologies that have been proved capable of inaccuracy and covert manipulation. The German court has articulated clear principles of constitutional law, well-fashioned for the new threats posed to contemporary democracy by seemingly benign information technologies. The critical question facing U.S. citizens is whether our courts will courageously rule in a scientifically sound manner to protect popular sovereignty when they face the impending questions concerning the constitutional sufficiency of the currently deployed electronic voting technologies.[164]

CONCLUSION

The national effort to upgrade voting technology and thus protect the right to vote has produced laudable improvements in the residual vote rate and more modestly in accessibility for disabled voters. But given the definitive voting technology assessments that issued in 2007, corrective responses are overdue. Where fundamental rights are concerned, governments are required to exercise special protective care. That high standard has been met by neither those state governments who continue to deploy all-electronic DRE voting systems, nor by most states that use electronic scanners. While litigation is not a first choice for resolving the impasse between advocates of recountable elections and government officers, the persistent misunderstandings regarding the gravity of the scientific findings may leave no alternatives but litigation.

More than ever, election policymakers and administrators need sufficient computer security training styled for their sensitive jobs so indicators of dangerous malfunctions that might affect vote totals will be understood and prompt effective remedial action. Given the grave cyber threats all governmental and private sector information systems are facing, the nation and its courts must confront the harsh realities about e-voting technology's failures thus far. Election law scholars must grapple with these realities as well to point the way forward for

[164] Cases pending currently include *Banfield v. Aichele*, Appeal of Motion for Partial Summary Judgment, Docket No. 442 M.D. 2006 (2011) (challenging the Pennsylvania constitutionality of the DRE voting systems that lack a paper audit trail); and *Gusciora v. Christie*, Docket No. A–005608–10T3 (Sup. Ct. N.J. 2011) (challenging the New Jersey state constitutionality of the DRE voting systems that lack a paper audit trail).

protecting constitutional voting rights from well-intended but misunderstood technical innovations.[165]

[165] Information system technologies pose a broad array of risks to constitutional rights and values. *See generally* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE (Jeffrey Rosen & Benjamin Wittes, eds. 2011) (exploring the impact of new technologies on privacy, identity, freedom from self-incrimination, genetic information, and other values). Election technologies could provide a prime example, but again, were sidestepped by major legal scholars.