THE RIGHT TO VOTE SECURELY

SUNOO PARK*

American elections currently run on outdated and vulnerable technology. Computer science researchers have shown that voting machines and other election equipment used in many jurisdictions are plagued by serious security flaws, or even shipped with basic safeguards disabled. Making matters worse, it is unclear whether current law requires election authorities or companies to fix even the most egregious vulnerabilities in their systems, and whether voters have any recourse if they do not.

This Article argues that election law can, does, and should ensure that the right to vote is a right to vote securely. First, it argues that constitutional voting rights doctrines already prohibit election practices that fail to meet a bare minimum threshold of security. But the bare minimum is not enough to protect modern election infrastructure against sophisticated threats. This Article thus proposes new statutory measures to bolster election security beyond the constitutional baseline, with technical provisions designed to change the course of insecure election practices that have become regrettably commonplace, and to standardize best practices drawn from state-of-the-art research on election security.

---

* Postdoctoral Fellow, Columbia University, and Visiting Fellow, Columbia Law School. JD, Harvard Law School. PhD in Computer Science, Massachusetts Institute of Technology. With gratitude to Alex Abdo, Kendra Albert, Katy Glenn Bass, Christopher Bavitz, Steven M. Bellovin, Jack Cable, Ran Canetti, Matthew Caulfield, Michael C. Dorf, Joseph Fishkin, James Grimmelmann, Joseph Lorenzo Hall, Douglas W. Jones, In-Uck Park, Filippo Raso, Blake E. Reid, Daniel C. Richman, Ronald L. Rivest, Aviel D. Rubin, Christopher Slobogin, Nicholas Spooner, Nicholas O. Stephanopoulos, David Vladeck, and participants in the Cornell Law Faculty Seminar (April 2022) and the CS+Law Virtual Seminar (May 2022) for their thoughtful feedback, and thanks to Aviel Menter for valuable research assistance. This research was supported in part by a Computing Innovation Fellowship, funded by the National Science Foundation under Grant #2127309 to the Computing Research Association and by the Cornell Tech Digital Life Initiative. The author has previously provided legal representation to Voting Village.

INTRODUCTION

Imagine it's a future Election Day. These days, voters can cast their votes during a quick lunch break—by simply filling out their ballot, folding the ballot into a paper airplane, and throwing it out of the nearest window. It's raining today, but no matter: modern ballots are made of a waterproof, metallic material that withstands rain, snow, or even getting run over by a car. Poll workers are patrolling the streets every couple of hours to collect the paper airplanes strewn over the ground and take them to a secure location for tallying. Each registered voter can obtain a ballot on or in advance of Election Day, so everyone has plenty of time to inform themselves about the issues on the ballot.

Some voters are expressing their appreciation on social media, thrilled at how modern technology has streamlined the voting process—increasing turnout and saving everyone time. But many are pushing back. Some are wondering about the odds that their ballot will make it to the secure tallying location and doubting how much to trust the outcome of this election. Some are questioning the meaning of increased turnout when it comes at the cost of meaningful assurance that cast votes will be counted. Some are asking: Is an election system that affords such potential for widespread alteration and disappearance of ballots after casting even legal?

In fact, it is alarmingly unclear whether and to what extent the U.S. Constitution or other laws permit *insecure* election systems that allow widespread ballot alteration or disappearance after casting—even in egregious cases like the paper airplane story. It is also unclear whether regular voters (or anyone else) would have standing to challenge such insecure election practices in court. It would be unlawful for the election system or election officials themselves to tamper with ballots—but the legal analysis enters more uncharted waters if the election system "merely" leaves the door wide open to ballot tampering by third parties. The problem is exacerbated if there is uncertainty about whether such tampering actually took place on a specific occasion. Ironically, such evidentiary problems are most likely to arise in cases involving the most lax security: if a door is wide open and unmonitored, then naturally, it is very hard to tell whether unauthorized access or tampering occurred.

The paper airplane story is, of course, far-fetched; an election system with such readily apparent and gaping omissions in its ballot security measures would not be taken seriously. But real election systems can and do have serious security problems, too—problems that are harder to detect, harder to explain, and harder to understand. This only makes the legal status of realistic election systems more difficult to ascertain since, as noted above, the availability of legal recourse is not clear-cut even in the face of readily apparent and egregious security flaws.

The last major congressional effort at modernizing voting technology was the Help America Vote Act (HAVA) of 2002, which aimed in part to address security concerns raised by the closely contested presidential election of 2000.[1] HAVA's well-meant provisions ultimately led to widespread adoption of "direct recording electronic" (DRE) voting technology[2] (often touchscreen machines), which was generally less secure than that which it replaced (often optical-scan or punch card ballots). Over the 2000s, extensive security research from many independent groups documented serious security vulnerabilities

1. Help America Vote Act (HAVA) of 2002, 52 U.S.C. §§ 20901–21145 (2023).

2. In DRE systems, "[v]oters use an electronic interface to record their votes directly into a computer's memory (e.g., onto a memory cartridge or memory card). That computer counts the vote." NAT'L ACADS. OF SCIS., ENG'G, & MED., SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY 41 (2018) [hereinafter NAS REPORT].

in these DRE machines.[3] Yet despite conclusive research findings, insightful reporting by journalists, and dedicated advocacy by many, reform has been slow and hard-won over years and achieved against vocal resistance.[4] Absent legal obligations on vendors or election officials to mitigate known, serious vulnerabilities in election equipment, and absent adequate funding and resources allocated to support such mitigation, well-documented security flaws in our election system have been gradually and arduously reduced, but not eliminated, over the course of well over a decade. This progress was in large part due to a move back towards basic, paper-based voting methods which either replaced or supplemented existing machines. To this day, election systems in some states still run on vulnerable post-HAVA technology.[5] In the meanwhile, proposals to adopt new insecure election technologies continue to crop up regularly and gain considerable traction.[6]

More recently, the issue of election security has regrettably been complicated, and sensationalized, by prominent unfounded claims of election rigging and widespread fraud in the 2020 presidential election, including by the outgoing president himself.[7] Baseless claims of election fraud should, of course, be treated and dismissed as such—as I discuss in more detail later.[8] At the same time, the prevalence of unfounded claims must not obscure the need to redress serious security concerns founded on scientific evidence; that is the focus of this Article.

---

3. *See, e.g.*, PATRICK MCDANIEL ET AL., EVEREST: EVALUATION AND VALIDATION OF ELECTION-RELATED EQUIPMENT, STANDARDS, AND TESTING (2007), https://www.eac.gov/sites/default/files/document_library/files/EVEREST.pdf [https://perma.cc/B2EW-A8GV] [hereinafter EVEREST REPORT]; Tadayoshi Kohno et al., *Analysis of an Electronic Voting System*, PROC. OF THE IEEE SYMPOSIUM ON SEC. & PRIVACY (2004); AGGELOS KIAYIAS ET AL., UNIV. OF CONN. VOTING TECH. RSCH. CTR., INTEGRITY VULNERABILITIES IN THE DIEBOLD TSX VOTING TERMINAL (2007); Joseph A. Calandrino et al., *Source Code Review of the Diebold Voting System*, *in* CAL. SEC'Y OF STATE TOP-TO-BOTTOM REVIEW (2007); DOUGLAS W. JONES & BARBARA SIMONS, BROKEN BALLOTS: WILL YOUR VOTE COUNT? 108–11, 159–87, 204–13 (2012).

4. *See generally* JONES & SIMONS, *supra* note 3.

5. *See infra* Part I.

6. *See infra* note 38.

7. *See, e.g.*, Donald J. Trump (@realDonaldTrump), TWITTER (Dec. 14, 2020, 2:59 PM), https://twitter.com/realDonaldTrump/status/1338574268154646528?cxt=HHwWgMCw7Y2NyZMlAAAA [https://perma.cc/LBS7-XDJU]; Donald J. Trump (@realDonaldTrump), TWITTER (Dec. 22, 2020, 10:29 AM), https://twitter.com/realdonaldtrump/status/1341405487057821698 [https://perma.cc/X4JX-FZ67].

8. *See infra* Part I, Section VI.B.

To date, litigation and legal theories around insecure election infrastructure have been sparse and uncoordinated. Scattered lawsuits challenging insecure election technology have put forward an assortment of legal theories with bases ranging from equal protection to state administrative provisions; they have seen mixed success.[9] Most recently, Georgia courts have considered a series of constitutional challenges to the state's use of outdated and insecure voting machines, in which the courts recognized plaintiffs' standing and indicated promisingly that courts may be open to granting injunctive relief; but courts have yet to clarify what constitutional doctrines properly apply to such challenges.[10] Legal academic commentary on the topic has been rarer yet,[11] and none has provided a comprehensive view of constitutional or legislative approaches to election infrastructure security.

This Article is the first to propose a unified constitutional theory of election system security, and the first to lay out a legislative approach based on an integrated view of the technological state of the art in election security and systems security. I develop a constitutional analysis of insecure election systems that comports with theories raised, but not elaborated or disambiguated, by scattered case law, and I conclude that election practices that fall egregiously short of a minimal threshold of security are likely unconstitutional under existing voting rights doctrines. Then I argue that, to bolster election security beyond the constitutional baseline, Congress should enact a statute providing federal standards and resources for securing election systems. In the traditionally highly

9. *See* Black v. McGuffage, 209 F. Supp. 2d 889 (N.D. Ill. 2002); Stewart v. Blackwell, 444 F.3d 843 (6th Cir. 2006); Wexler v. Anderson, 452 F.3d 1226 (11th Cir. 2006); Banfield v. Cortes, 110 A.3d 155 (Pa. 2015); *infra* note 10.

10. *See* Curling v. Kemp, 334 F. Supp. 3d 1303 (N.D. Ga. 2018); Curling v. Raffensperger (*Raffensperger I*), 2020 WL 5757809 (N.D. Ga. Sep. 28, 2020); Curling v. Raffensperger (*Raffensperger II*), 2020 WL 5994029 (N.D. Ga. Oct. 11, 2020).

11. *See* Candice Hoke, *Judicial Protection of Popular Sovereignty: Redressing Voting Technology*, 62 CASE W. L. REV. 997 (2012); Paige Reinauer, *From Hanging Chads to Data Hacks: Maintaining Election Integrity in the Digital Age*, 14 J. BUS. & TECH. L. 533 (2019); Andrew W. Appel & Philip B. Stark, *Evidence-Based Elections: Create a Meaningful Paper Trail, Then Audit*, 4 GEO. L. TECH. REV. 523 (2020); Stephanie Phillips, Note, *The Risks of Computerized Election Fraud: When Will Congress Rectify a 38-Year-Old Problem?*, 57 ALA. L. REV. 1123 (2006); Jacob Rush, Note, *Hacking the Right to Vote*, 105 VA. L. REV. ONLINE 67 (2019); Jennifer Nou, Note, *Privatizing Democracy: Promoting Election Integrity Through Procurement Contracts*, 118 YALE L.J. 744 (2009).

decentralized domain of election administration, this legislation would provide a framework for state and local election officials to continue to manage and secure election infrastructure locally while drawing on federal funding and resources.

This Article proceeds in six parts. Parts I, II, and III offer historical, technical, and legal background, respectively. Part I overviews HAVA's history and aftermath, voting technology and security improvements since HAVA, and relevant politics of election security today. Part II provides background on election systems and a technical overview of the problem of *securing* election infrastructure, drawing in depth upon the computer science literature on election security. It presents a novel formulation of election system security in terms of three requirements ("casting, counting, and checking"), which succinctly captures key considerations for election law. Part III overviews the relevant election law, including constitutional right-to-vote doctrines and election administration legislation.

Parts IV and V then develop my constitutional analysis and legislative proposals, and Part VI addresses potential concerns about the ideas in Parts IV and V. Part IV considers how the constitutional right to vote implies a right to vote securely. It analyzes whether providing insecure election infrastructure amounts to a constitutional violation under existing voting-rights doctrines. The analysis concludes that the use of sufficiently insecure election systems can (1) unconstitutionally burden voting rights and (2) unconstitutionally cause arbitrary and disparate treatment of similarly situated voters. However, for a variety of reasons, constitutional litigation is a poor vehicle for *realizing* robust election security. Part V thus sets out a legislative approach that can provide a more reliable foundation for election security, proposing detailed measures that new federal election legislation should include to enhance election security beyond baseline constitutional guarantees. It particularly focuses on transparency and auditability measures to ensure robust security when modern digital technology is built into critical election infrastructure. Part VI then considers several potential concerns that might be raised in response to the preceding ideas and discusses: (1) the importance of promoting access and security as complementary, not opposing, values; (2) unfounded speculations of election fraud, such as those promoted by Donald J. Trump supporters in 2020, and how they are readily distinguishable from legitimate challenges to insecure election infrastructure; and (3) the need for technical,

legal, and political approaches to address the problem of election insecurity and lack of public confidence in elections.

I. HISTORICAL BACKGROUND

HAVA[12] was passed in the wake of the controversial election of 2000. Among other things, HAVA responded to concerns about the reliability of election technology raised in the contested Florida presidential race.[13] By the official tally, George W. Bush won Florida by just 537 votes among six million cast,[14] bringing a national spotlight to certain unreliable features (such as "hanging chads")[15] of the punch card ballot technology then used. This unreliability had been well-documented for over a decade,[16] but no mitigations had been made, perhaps because no election in memory had been close enough for the ballots' unreliability to cast serious doubt on the outcome. But Florida in 2000 was that close, and the presidency was at stake.

The parties rushed to court, and the Supreme Court's *Bush v. Gore*[17] decision meant the original tally was certified without completing a recount. Long story short, Bush became president, and reforming election procedures and technology became a national legislative priority.

HAVA passed two years later and soon afterward led to widespread adoption of DRE voting technology (often touchscreen machines) that was less secure than many of the older systems it replaced.[18] This ill-fated technological reform was due in part to incomplete understanding of the complex security implications of electronic voting systems, alongside legitimate discontent with existing technology.[19] Such post-HAVA complications, along with the fact that no similarly

12. HAVA, 52 U.S.C. §§ 20901–21145 (2023).

13. *See* JONES & SIMONS, *supra* note 3, at 141–47.

14. Michael Levy, *United States Presidential Election of 2000*, ENCYC. BRITANNICA, https://www.britannica.com/event/United-States-presidential-election-of-2000 [https://perma.cc/WT3C-QJXT] (Dec. 15, 2022).

15. *See* Douglas W. Jones, *Chad—From Waste Product to Headline*, UNIV. OF IOWA DEP'T OF COMPUT. SCI., https://homepage.divms.uiowa.edu/~jones/cards/chad.html [https://perma.cc/5EB4-Z69R] (Jan. 2006).

16. ROY G. SALTMAN, NAT'L BUREAU OF STANDARDS INST. FOR COMPUT. SCIS. & TECH., ACCURACY, INTEGRITY, AND SECURITY IN COMPUTERIZED VOTE-TALLYING 5, 30–36, 111 (1988).

17. 531 U.S. 98 (2000).

18. *See generally* JONES & SIMONS, *supra* note 3.

19. *See infra* note 192.

scoped election legislation has been passed in the two decades since, are one indication of the challenges of election system reform—and of the extent to which legislation may be outpaced by technological change.

To this day, election systems in many states run on post-HAVA technology that is vulnerable—and not just to sophisticated, costly attacks. Over decades, research on the security of voting machines and other election equipment has shown a "uniform[] fail[ure] to adequately address important threats against election data and processes."[20] Incredibly, multiple investigations have found that voting machines and other equipment "are shipped with basic security features disabled"[21] and "fail[] to follow standard and well-known [security] practices,"[22] opening the door to inexpensive, unsophisticated attacks that might be considered the digital equivalent of tampering with ballots in an unlocked, unmonitored place.

Take, for example, Voting Village, an event at a major computer security conference called DEF CON.[23] Voting Village's findings are dismaying and sadly not novel; the findings reconfirm the kinds of problems that researchers have documented for decades.[24] In 2019, Voting Village participants examined a range of election equipment, most of which were device models in use in more than fifteen states, and all of which were models "currently certified for use in at least one U.S. jurisdiction."[25] As in preceding years, using surprisingly basic techniques, "participants were able to . . . compromis[e] every . . . device[] in the room in ways that could alter stored vote tallies, change ballots displayed to voters, or alter the internal software

20. EVEREST REPORT, *supra* note 3, at 3; *see also* sources cited *supra* note 3.

21. MATT BLAZE ET AL., DEF CON 27 VOTING MACHINE HACKING VILLAGE 27 (2019), https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf [https://perma.cc/A9E7-2ZPY] [hereinafter VOTING VILLAGE 2019].

22. EVEREST REPORT, *supra* note 3, at 3; NAS REPORT, *supra* note 2, at 89.

23. VOTING VILLAGE 2019, *supra* note 21, at 3.

24. Voting Village's findings are largely not original; the event's focus has been on raising awareness of the security issues in election technology and reconfirming prior security research. Some of the Voting Village demonstrations may be criticized for sensationalizing previously known vulnerabilities disproportionately to their likely impact. The Voting Village reports provide, however, an illustrative and recent recap of the types of problems that security researchers have documented over the years and, as such, are a useful summary source spanning original research performed by many others. *See* sources cited *supra* note 3.

25. VOTING VILLAGE 2019, *supra* note 21, at 4, 8–10.

that controls the machines."[26] As an illustration, the participants reprogrammed some machines entirely, modifying them to play video games and to display a popular internet meme called Nyan Cat.[27] While such demonstrations may seem whimsical, some of the same techniques could enable reprogramming to surreptitiously alter how a machine tallies votes in a real election.[28]

The extent of election systems' reliance on the machines has decreased significantly over the last two decades. Notably, (1) the fully electronic voting machines that were widely used in the 2000s have, in most states, been replaced or at least supplemented by more secure voting methods that provide a paper audit trail,[29] and (2) post-election audits to independently verify machine-generated tallies have become more common, and are even mandated by law in a growing minority of states.[30] Those vulnerable machines that are still in use have, in some states, been retrofitted with ballot printers that make audits possible.[31] Auditing and other election procedures have improved in sophistication and frequency, significantly reducing the likelihood of errors or surreptitious compromise going undetected.[32]

---

26. *Id.* at 4.

27. *Id.* at 19, 22; *see also* Nyan Cat, *Nyan Cat [original]*, YOUTUBE (Apr. 5, 2011), https://www.youtube.com/watch?v=QH2-TGUlwu4 [https://perma.cc/N5B6-2L9N] (depicting a pixelated cat, with a Pop Tart shaped body, flying through a starry night sky with a waving rainbow banner in its wake, accompanied by an energetic theme tune).

28. VOTING VILLAGE 2019, *supra* note 21, at 18–22; *see also* Lily Hay Newman, *Some Voting Machines Still Have Decade-Old Vulnerabilities*, WIRED (Sep. 26, 2019), https://www.wired.com/story/voting-village-results-hacking-decade-old-bugs [https://perma.cc/M2DY-GQ8Q].

29. *See infra* Figure 1; *infra* note 37.

30. *See Post-Election Audits*, NAT'L CONF. STATE OF LEGISLATURES, https://www.ncsl.org/elections-and-campaigns/post-election-audits [https://perma.cc/W6DB-2EKU] (Sept. 22, 2022) [hereinafter *2022 NCSL Post-Election Audits*].

31. *See* JONES & SIMONS, *supra* note 3, at 113–14; STAFF REPORT, NAPA CNTY. VOTING MODERNIZATION BD., VVPAT RETROFIT - CHANGE TO APPROVED PROJECT DOCUMENTATION PLAN (2006), https://elections.cdn.sos.ca.gov/vma/pdf/vmb/documents/staff_reports/napaplanchange_vvpat_staffreport.pdf [https://perma.cc/2PE5-FLZ6].

32. *Compare 2022 NCSL Post-Election Audits*, *supra* note 30, *with* Archive of *Post-Election Audits*, NAT'L CONF. OF STATE LEGISLATURES (Mar. 11, 2016), https://web.archive.org/web/20160417021544/https://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx [https://perma.cc/TG2R-SM4K].

Despite well-known research documenting the serious security flaws of paperless DRE machines in the 2000s,[33] change has been slow and is still ongoing, as summarized in Figure 1. Due to financial and other practical constraints, many vulnerable twenty-year-old machines remain in active, though limited, use, with their security shored up by procedural safeguards (e.g., originally purely electronic machines retrofitted to produce paper records alongside).

The reforms thus far are the fruits of long years of advocacy against vocally resistant opposing interests. Voting machine companies (in an oligopoly market[34]) have been known to brush aside vulnerability reports and threaten security researchers with legal action or attack their motives, rather than fixing problems.[35] Voting machines are expensive for states to buy, upgrade, and replace,[36] and concerns about reputation and voter confidence can create counterproductive pressures to double down on past election management decisions rather than publicizing and implementing costly mitigation of mistakes. The absence of legal obligations to mitigate known election system vulnerabilities further slows the pace of change and tends to result in highly discretionary and localized reform.

Figure 1. Reduction in vulnerable election infrastructure, 2008–2020[37]

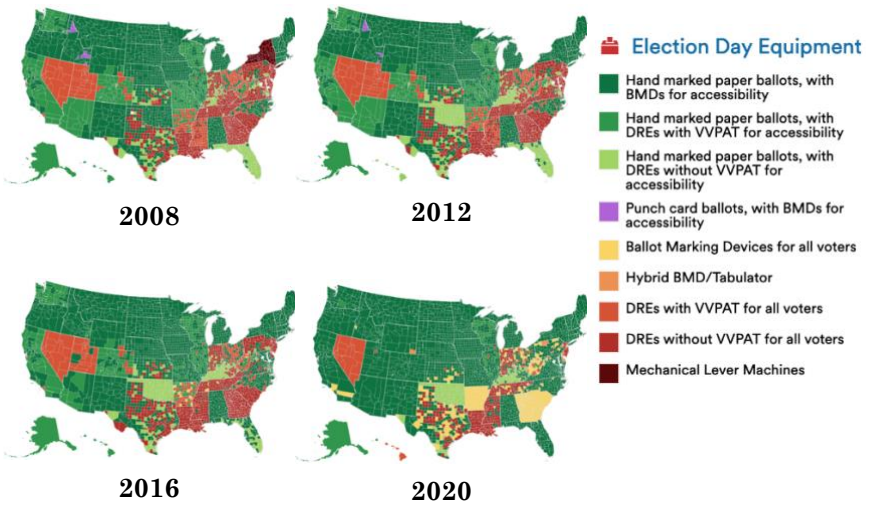
33. *See* sources cited *supra* note 3.

34. *See* MATTHEW CAULFIELD ET AL., THE PRICE OF VOTING: TODAY'S VOTING MACHINE MARKETPLACE 8–13 (2021).

35. *See* Andrew Appel, *ESS Voting Machine Company Sends Threats*, FREEDOM TO TINKER (Jan. 11, 2021), https://freedom-to-tinker.com/2021/01/11/ess-voting-machine-company-sends-threats [https://perma.cc/SKS7-UZH4]; Declan McCullagh, *Sequoia Warns Princeton Professors over E-voting Analysis*, CNET (Mar. 18, 2008), https://www.cnet.com/news/sequoia-warns-princeton-professors-over-e-voting-analysis [https://perma.cc/689U-UWS7]; AVIEL D. RUBIN, BRAVE NEW BALLOT: THE BATTLE TO SAFEGUARD DEMOCRACY IN THE AGE OF ELECTRONIC VOTING 69 (2006).

36. *See* Sarah Breitenbach, *Aging Voting Machines Cost Local, State Governments*, PEW (Mar. 2, 2016), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/03/02/aging-voting-machines-cost-local-state-governments [https://perma.cc/UZ6N-DGZL].

37. *The Verifier—Election Day Equipment*, VERIFIED VOTING (Nov. 2022), https://verifiedvoting.org/verifier [https://perma.cc/FZ7E-385N]; *see also infra* Part II (explaining the technologies listed).



Finally, despite the hard-won progress to date, proposals to adopt new insecure election technology—some of which security researchers have been warning against for years—are made regularly and often gain considerable traction.[38] Some have already been used for pilot programs, as well as limited overseas

38. *See* Michael A. Specter et al., *The Ballot Is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections*, PROC. OF USENIX SEC. SYMP. 1535 (2020); TRAIL OF BITS, VOATZ: SECURITY ASSESSMENT (2020), https://github.com/trailofbits/publications/blob/master/reviews/voatz-securityreview.pdf [https://perma.cc/9DSA-2FGS]; Scott Wolchok et al., *Attacking the Washington, D.C. Internet Voting System*, PROC. OF FIN. CRYPTOGRAPHY 114 (2012); Remote Accessible Vote by Mail Systems, S.B. 1480, 2021-2022 Reg. Sess. (Ca. 2022); Benjamin Freed, *Rhode Island Governor Signs Bill Allowing Internet Voting*, STATESCOOP (July 5, 2022), https://statescoop.com/rhode-island-governor-signs-bill-allowing-internet-voting [https://perma.cc/LT89-78WW]; John Marion & Pamela Smith, *Letter to Rhode Island Governor Urging Veto of Bills That Allow the Online Return of Voted Ballots*, VERIFIED VOTING (June 28, 2022), https://verifiedvoting.org/letter-to-ri-governor-internet-voting-6-28-22 [https://perma.cc/D6T3-H9GL]; Benjamin Freed, *Utah County, Utah, Begins Review of Mobile-App Votes*, STATESCOOP (Sept. 4, 2019), https://statescoop.com/utah-county-utah-begins-review-of-mobile-app-votes [https://perma.cc/3NNE-S43Q]; Benjamin Freed, *Denver to Test Blockchain-Encrypted Mobile Voting in May Election*, STATESCOOP (Mar. 7, 2019), https://statescoop.com/denver-to-test-blockchain-encrypted-mobile-voting-in-may-election [https://perma.cc/5AUM-A6VU]; Benjamin Freed, *Mobile Voting Arrives for 1.2 Million Seattle-Area Voters*, STATESCOOP (Jan. 22, 2020), https://statescoop.com/mobile-voting-arrives-seattle-washington [https://perma.cc/45YR-SMMX]; Barbara Simons, *Why Internet Voting Is Dangerous*, 4 GEO. L. TECH. REV. 543 (2020).

and military voting in federal elections.[39] Such proposals are often buoyed by the relatable promise of modernity, convenience, and cost efficiency, beside which their security risks may initially appear secondary, especially to those without the expertise to assess the risks' severity firsthand.

* * *

Today, following the controversial elections of 2016 and 2020, election security is once again near the forefront of U.S. public consciousness and has become an increasingly politicized topic.

In recent decades, claims of election insecurity have often been associated with the politically charged issue of limiting access to elections. But as a member of Congress aptly put it, "[e]veryone agrees that we should make it easier to vote . . . and we should make it harder to cheat."[40] Access and security are not only compatible; neither is meaningful without the other. Achieving both simultaneously is an important and challenging goal for election policy to work toward.[41]

The 2019 release of the nonpartisan Mueller Report, documenting attempted Russian influence on the 2016 U.S. presidential election,[42] cast a new national spotlight on election security. To some, the Mueller Report underscored the strong incentives for sophisticated adversaries to attack the U.S. election system and the importance of strengthening the system's security in the future. To others, the Mueller Report confirmed that neither the president nor Russia hacked the 2016 presidential election, with the takeaway that the current system is working well.

---

39. *See* sources cited *supra* note 38.

40. David Nather, *Election Overhaul May Have to Wait in Line Behind Other 'Crisis' Issues*, CQ WEEKLY 2034 (July 27, 2002) (quoting Representative Steny Hoyer).

41. *See infra* Section VI.A (arguing that access and security are compatible and complementary); Andrea Córdova McCadney et al., *2020's Lessons for Election Security*, BRENNAN CTR. FOR JUST. (Dec. 16, 2020), https://www.brennancenter.org/our-work/research-reports/2020s-lessons-election-security [https://perma.cc/QG86-HG8C] ("Election security promotes voter access, and voter access promotes security.").

42. ROBERT S. MUELLER III, U.S. DEP'T OF JUST., REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION (2019) [hereinafter MUELLER REPORT].

In 2020, Trump and his supporters instilled a deep distrust of the election system among a significant segment of the electorate leading up to the presidential election. Following the election, they spread unfounded allegations of widespread fraud and claimed that the election was "stolen."[43] Trump even cited Voting Village and other security research as supposed support for these claims.[44] Trump's supporters took their claims to courts across the country, which consistently ruled against every one of hundreds of lawsuits based on such allegations.[45]

The Department of Homeland Security (DHS) responded with a public statement that the 2020 election was "the most secure in American history,"[46] which was corroborated with statements of confidence from the Department of Justice, the Federal Bureau of Investigation (FBI), and the Election Assistance Commission (EAC), as well as numerous state and local election officials.[47] These statements, confirming the Republican loss in the 2020 election, came overwhelmingly from Republican officials.[48]

Over fifty prominent security researchers, many of whom have studied and criticized security weaknesses in election equipment for decades, also responded publicly: "We are aware of alarming assertions being made that the 2020 election was 'rigged' by exploiting technical vulnerabilities. However, in every case of which we are aware, these claims either have been

---

43. *See* sources cited *supra* note 7; JOHN DANFORTH ET AL., LOST, NOT STOLEN: THE CONSERVATIVE CASE THAT TRUMP LOST AND BIDEN WON THE 2020 PRESIDENTIAL ELECTION (2022), https://lostnotstolen.org [https://perma.cc/89HG-YYHV].

44. *See* Joseph Marks & Tonya Riley, *The Cybersecurity 202: Trump's Finally Talking About Election Security – But Only to Spread Conspiracy Theories*, WASH. POST (Nov. 16, 2020, 7:19 AM), https://www.washingtonpost.com/politics/2020/11/16/cybersecurity-202-trumps-finally-talking-about-election-security-only-spread-conspiracy-theories [https://perma.cc/EPC9-EQA9].

45. *See infra* Section VI.B (discussing such baseless claims, and how they are distinguishable from claims of election security based on established scientific evidence, in more detail).

46. *Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Nov. 12, 2020), https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election [https://perma.cc/29DG-75L4].

47. *See It's Official: The Election Was Secure*, BRENNAN CTR. FOR JUST. (Dec. 11, 2020), https://www.brennancenter.org/our-work/research-reports/its-official-election-was-secure [https://perma.cc/XE4P-3AUU].

48. *See id.*

unsubstantiated or are technically incoherent."[49] Citing such research to back up claims of fraud fundamentally misunderstands the research, as they explained: "Merely citing the existence of technical flaws does not establish that an attack occurred, much less that it altered an election outcome."[50]

The recent trend of misinformation about election integrity poses a threat to U.S. democracy that will only be exacerbated by a continued failure to take security flaws in election equipment seriously. The 2020 election *was* the most secure in history, but some states are still using twenty-year-old machines with known vulnerabilities, some states are not conducting robust post-election audits, and some states are seriously considering once again replacing their outdated election equipment with new technology that is even less secure. Now more than ever, it is important to strengthen our election infrastructure to be robust not only against any fraud that might occur, but also against the alleged levels of widespread fraud that many ardently believe exist. It is furthermore urgent to establish a robust legal framework to provide procedural protections for the security of U.S. election infrastructure into the future and offer legal recourse against too-insecure systems, while systematically distinguishing and dismissing baseless claims of election fraud.

It is difficult at times to separate election security from the turbulent politics engulfing it. But at its core, election security is not a partisan issue; "insecure and unreliable elections threaten everybody, without regard to party or ideology."[51] In a democracy, it is in all parties' interests to prevent technological manipulation of elections, to ensure an election's true winner is the one elected, and to promote public confidence in elections. But even through a cynical lens of pure partisanship where each party's interest is simply to win, when faced with insecure election infrastructure, all parties should be similarly concerned, as one cannot know whether a hacker's allegiance will be with one party, the other, or a foreign power. It is in nobody's interest that the election be decided by whichever gang of hackers prevails.

---

49. Tony Adams et al., *Scientists Say No Credible Evidence of Computer Fraud in the 2020 Election Outcome, But Policymakers Must Work with Experts to Improve Confidence*, MATT BLAZE'S EXHAUSTIVE SEARCH (Nov. 16, 2020), https://www.mattblaze.org/blog/election-letter [https://perma.cc/N5Q7-RAS3].

50. *Id.*

51. RUBIN, *supra* note 35, at 43.

II. WHAT IS A SECURE ELECTION SYSTEM?

Election system security is a special case of system security.[52] System security "is about building systems to remain dependable in the face of malice, error, or mischance."[53] Security professionals recognize that no system behaves perfectly at all times;[54] thus, a secure system is one that behaves reliably as intended—not always, but as much of the time as reasonably possible, even under unexpected circumstances or when subjected to adversarial attacks. If and when a secure system fails, it should do so *detectably* so that the people who depend on it are not lulled into false complacency even though something has gone wrong, and so that the results of the failure can be treated appropriately (and ideally, redressed).

In any particular context, "robust security design requires that the . . . goals [(i.e., intended behavior and failure modes)] are made explicit."[55] What does this mean for elections? An election is "a process in which [eligible] people vote to choose a person or group . . . to hold an official position,"[56] or to choose a decision to be taken. The specifics of voter eligibility and methods of choice among candidates (or outcomes) will vary from jurisdiction to jurisdiction, office to office, and election to election. As such, election security is a *procedural* property. A

52. Election system security is also a subcategory of election security. The latter additionally encompasses concerns unrelated to the functioning of election systems, which could nonetheless impact election integrity, such as manipulative misinformation on social media or voter harassment. This Article focuses primarily on election system security, not election security more broadly.

53. ROSS ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS 3 (3d ed. 2020).

54. From the perspective of the security community, a system that is claimed to behave perfectly correctly in all circumstances, rather than being considered secure, would be regarded with skepticism and as exceeding credibility. Recognizing human fallibility and the implausibility of building perfect systems, best practices in security call for guarantees of *either* correct behavior *or* reliable, detectable failure modes that ideally provide insight into what failed and how it can be fixed. JOHN VIEGA & GARY MCGRAW, BUILDING SECURE SOFTWARE: HOW TO AVOID SECURITY PROBLEMS THE RIGHT WAY 97 (2002) ("Any sufficiently complex system has failure modes. Failure is unavoidable and should be planned for. What *is* avoidable are security problems related to failure."); NAS REPORT, *supra* note 2, at 88–89 ("[C]ybersecurity is a concern with all computer systems. This is because . . . the design and development of current computer systems, no matter how well constructed, cannot anticipate and prevent all the possible means of attack . . . .").

55. ANDERSON, *supra* note 53, at 16.

56. *Election*, COLLINS DICTIONARY, https://www.collinsdictionary.com/dictionary/english/election [https://perma.cc/3UVW-GKGG].

secure election is one in which the applicable substantive rules[57]—whatever they are—are accurately and verifiably followed. The basic intended behavior of an election system is to aggregate the electoral preferences of eligible voters and produce a list of elected candidates (or decisions) as determined by those preferences according to applicable substantive rules, and a *secure* election system is one that either performs this function or fails detectably.

What does it take for an election system to be secure, as described above? There is no standard and comprehensive definition of election system security, covering all parts of an election system, that is collected in one authoritative place.[58] However, there is a core set of concepts to which research, policy, legislative, and media discourse about election system security consistently refers. I propose a three-part characterization of election system security, incorporating these core concepts.

A secure election system must provide reliable guarantees that (1) every eligible voter, and nobody else, has a meaningful opportunity to cast exactly one vote for the outcome of their true preference; (2) the reported election outcome accurately reflects the votes cast by eligible voters;[59] and (3) in case, for whatever reason, the preceding two requirements are not met, the system clearly and reliably produces evidence of its failure, checkable by

57. From the point of view of public policy, an election is procedural, but from the point of view of running the election, the rules on eligibility and aggregation are substantive. In all cases, these eligibility and aggregation rules will (or should) be publicly stated as binding law, as part of the system of government in which an election occurs.

58. For instance, modern expert commentary discussing the security of various aspects of election systems does not reference any standard comprehensive definition. *See* NAS REPORT, *supra* note 2; THE CTR. FOR INTERNET SEC., A HANDBOOK FOR ELECTIONS INFRASTRUCTURE SECURITY (2018) [hereinafter CIS HANDBOOK]; BELFER CTR. FOR SCI. AND INT'L AFFAIRS, HARV. KENNEDY SCH., THE STATE AND LOCAL ELECTION CYBERSECURITY PLAYBOOK (2018) [hereinafter HKS CYBERSECURITY PLAYBOOK]; Philip B. Stark & David A. Wagner, *Evidence-Based Elections*, 10 IEEE SEC. & PRIV. 33 (2012). One contributing factor is that election systems encompass such a range of different systems. *See infra* Section II.A.

59. By election outcome, I mean the winning candidate or decision, not the precise tally of votes. Assuring a correct tally is much harder and less realistic than assuring a correct outcome. For example, if there is a one in a million chance of miscounting each ballot in a population of 100 million, and the true tally is 52 and 48 million votes for Candidates A and B respectively, the likelihood of an incorrect reported *tally* would be more than 99.995 percent, but the likelihood of an incorrect reported *winner* would be far less than 0.000001 percent. This calculation assumes independence between ballots, which is unlikely to hold in practice. Still, it provides useful intuition for the difference between assuring a correct tally and assuring a correct outcome.

all interested parties (i.e., the electorate). The third guarantee implies *credible public assurance* of the preceding two guarantees by ensuring that any errors or tampering will be publicly evidenced.[60]

I call these the *casting* guarantee, the *counting* guarantee, and the *checking* guarantee. The three-part characterization of election security as casting, counting, and checking is an oversimplification, but it is a useful one that succinctly captures the key elements of election system security that election law is generally concerned with. It comports with existing scholarship and policy statements, including those with more technical detail than my definition offers,[61] and implies well-established requirements such as ballot secrecy (as detailed below).[62]

Next, Section II.A overviews the many parts of an election system. Section II.B describes the casting-counting-checking framework in more detail. Section II.C explains the security properties of traditional paper-ballot-based election systems in each of the three aspects. Section II.D explains some key points where introducing complex modern technology into election infrastructure may create new security risks not present in traditional paper-based systems, and on the other hand, notable areas where new technology promises to enhance security. Section II.E then describes how paper ballots can provide strong security guarantees, even in machine-tallied election systems. Finally, Section II.F overviews key differences between potential risk, realized risk, and magnitude of risk from security vulnerabilities.

A. What Is an Election System?

The term "election system" (or "election infrastructure") encompasses a broad range of infrastructure that is used in the

60. Advocates of "evidence-based elections" have long emphasized the importance of such evidence. *See* NAS REPORT, *supra* note 2, at 94; Stark & Wagner, *supra* note 58; Ronald L. Rivest & Philip B. Stark, *When Is an Election Verifiable?*, 15 IEEE SEC. & PRIV. 48 (2017); Appel & Stark, *supra* note 11.

61. *See* NAS REPORT, *supra* note 2; CIS HANDBOOK, *supra* note 58; *Recommendations to Defend America's Election Infrastructure*, BRENNAN CTR. FOR JUST. (Oct. 23, 2019), https://www.brennancenter.org/our-work/research-reports/recommendations-defend-americas-election-infrastructure [https://perma.cc/CAY9-AK3Y] [hereinafter *Brennan Ctr. Recommendations*]; HKS CYBERSECURITY PLAYBOOK, *supra* note 58; Simons, *supra* note 38; Stark & Wagner, *supra* note 58.

62. *See infra* Section II.B.

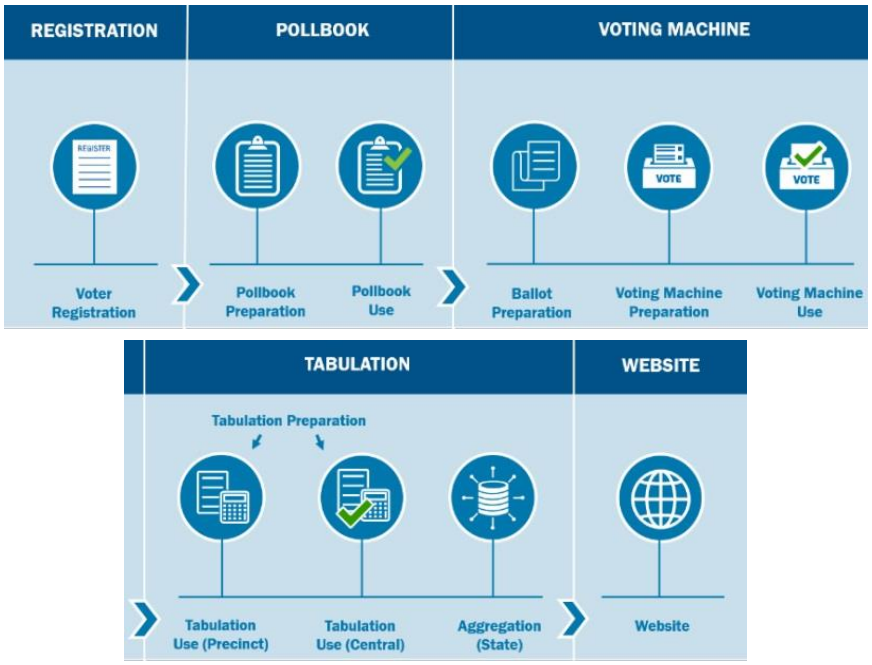
operation of elections, starting from voter identification and registration all the way to reporting of election results and post-election auditing: "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, . . . technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments."[63] For our purposes, election infrastructure comprises all the "systems [that] collect, process, and store data related to all aspects of election administration,"[64] and procedures associated with the use of those systems. In the United States, tallying is completed by machine except when special circumstances call for a hand recount.[65]

63. *Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector*, DEP'T OF HOMELAND SEC. (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical [https://perma.cc/MQK3-SYHK] [hereinafter *DHS Statement*].

64. NAS REPORT, *supra* note 2, at 34.

65. The prevalence of automation in American vote casting and tallying is relatively unusual and has been driven by the "large number of elections and . . . numerous contests on many ballots [which] create an [unusual] administrative challenge." *Id.* at 33. For example, many countries routinely count ballots by hand, a much simpler prospect in parliamentary systems with just a few choices on each ballot, compared to the United States where comprehensive manual counting has long been considered prohibitively complex and costly. *See* Chris Game, *Explainer: How Britain Counts Its Votes*, CONVERSATION (May 7, 2015), https://theconversation.com/explainer-how-britain-counts-its-votes-41265 [https://perma.cc/ZHC6-ZX8N]; Tyler Bloomfield, *Why Elections Canada Still Uses Paper Voter Lists and Hand Counts Ballots for Federal Elections*, CBC NEWS (Sept. 9, 2021), https://www.cbc.ca/news/politics/ask-paper-voter-lists-hand-counting-ballots-election-1.6167809 [https://perma.cc/7VU5-WKGR]; *Fonctionnement d'un Bureau de Vote*, MINISTÈRE DE L'INTÉRIEUR (2011), https://www.interieur.gouv.fr/Elections/Comment-voter/Fonctionnement-d-un-bureau-de-vote [https://perma.cc/L6LE-ACYL]; Sewell Chan, *Fearful of Hacking, Dutch Will Count Ballots by Hand*, N.Y. TIMES (Feb. 1, 2017), https://www.nytimes.com/2017/02/01/world/europe/netherlands-hacking-concerns-hand-count-ballots.html [https://perma.cc/D8QL-J4SB].

Figure 2. Functional overview of a U.S. election ecosystem (not comprehensive)[66]



In 2017, the DHS designated election systems as critical infrastructure, calling them "vital to our national interests" and noting that "cyber attacks on this country are becoming more sophisticated, and bad cyber actors—ranging from nation states, cyber criminals and hacktivists—are becoming more . . . dangerous."[67]

Figure 2 shows a "functional overview" of an election process in the United States, designed by the Cybersecurity & Infrastructure Security Agency (CISA) which encompasses many (but not all) components of election systems. The most informative conceptualization of election systems varies by context. For voters, for example, most activity is on election day; but for election administrators, election day activity is but a

66. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, ELECTION INFRASTRUCTURE CYBER RISK ASSESSMENT (2020), https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf [https://perma.cc/5LAE-DPDH] [hereinafter CISA ELECTION RISK ASSESSMENT].

67. *DHS Statement*, *supra* note 63; *see also* NAS REPORT, *supra* note 2, at 117–18 (discussing the implications of the critical infrastructure designation).

small part of a much longer process.[68] Many different types of technology as well as human processes are involved in election systems.

B. Casting-Counting-Checking Framework of Election System Security and the CIA Triad

Often, security is broken down into three essential components using the acronym "CIA," which stands for confidentiality, integrity, and availability.[69] CISA summarizes the CIA triad as follows: *confidentiality* attacks involve unauthorized "theft of information"; *integrity* attacks involve unauthorized "changing of either the information within or the functionality of a system"; and *availability* attacks involve "the disruption or denial of the use of the system."[70]

By considering what CIA requirements are necessary to effectuate the casting, counting, and checking guarantees specific to election systems, we can identify more concrete operational requirements that the systems must satisfy to be considered secure. Next, I explain how analyzing the casting-counting-checking framework with the CIA triad in mind yields a range of concrete properties widely considered important for election security.

Casting and confidentiality. Consider *ballot secrecy*, for example, a confidentiality guarantee considered essential in modern elections. Why is it considered so important to keep secret how people vote? After all, much information involved in the election process is deliberately made public for transparency reasons.

The U.S. Supreme Court put it this way: "A widespread and time-tested consensus demonstrates that [ballot secrecy] is necessary in order to serve . . . compelling interests in preventing voter intimidation and election fraud."[71] Election security scholars in computer science (including myself) have summarized it like this: "Protecting ballot secrecy provides a

68. *See* Douglas W. Jones, *Perspectives on Electronic Voting*, *in* FROM POWER OUTAGES TO PAPER TRAILS: EXPERIENCES IN INCORPORATING TECHNOLOGY INTO THE ELECTION PROCESS 27, 31–40 (2007).

69. *See* NAT'L RSCH. COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE 52 (1991); Jerome H. Saltzer & Michael D. Shroeder, *The Protection of Information in Computer Systems*, 63 PROC. OF THE IEEE 1278, 1280 (1975).

70. CISA ELECTION RISK ASSESSMENT, *supra* note 66.

71. Burson v. Freeman, 504 U.S. 191, 206 (1992).

strong and simple protection against coercion and vote selling: if you cannot be sure how anyone else voted, this removes your incentive to pay them or threaten them to vote the way you'd like."[72] And, corroborating this from a historical perspective, election law scholars have noted that "[b]ribery of voters was far and away the greatest impediment to the integrity of elections before the introduction of the secret ballot, a fact well known not only to historians but to readers of great 19th century fiction."[73]

As such, the secret ballot is an indirect yet crucial consequence of the *casting* guarantee's requirement that voters must have a meaningful opportunity to cast exactly one vote for the outcome of their true preference. Without ballot secrecy, voters could be coerced or persuaded to cast votes for an outcome that does not correspond to their true preference—a serious threat to the legitimacy of a democratic election. Many states impose other confidentiality requirements in addition to ballot secrecy (e.g., on voter information or partial tallies).

Casting. To ensure that only eligible voters can cast a vote, and that all eligible voters can cast a vote, voter registration information must be kept up-to-date and protected from unauthorized modification. To ensure that nobody can vote more than once in an election, there must be a reliable way of checking whether someone has already voted. And to ensure that recorded votes express the voter's intention, voters must have an opportunity to check their ballot and verify its contents before casting.

Ensuring that all eligible voters have a meaningful opportunity to cast a vote requires that the means of voting must be accessible to all eligible voters with low cost and effort throughout the allowed voting period. As previously noted, accessibility is sometimes seen as a separate issue from security, or even portrayed as in tension with security.[74] But in fact, the availability prong of the standard CIA triad means that ensuring accessibility for all intended users—even in the face of adversarial attacks—is a fundamental goal of securing any system, including election systems.

72. Sunoo Park et al., *Going from Bad to Worse: From Internet Voting to Blockchain Voting*, 7 J. CYBERSECURITY 1, 3 (2021).

73. DANIEL HAYS LOWENSTEIN ET AL., ELECTION LAW: CASES AND MATERIALS 458 n.a (6th ed. 2017) (referencing Charles Dickens's *Bleak House*, George Eliot's *Felix Holt, Radical*, and Anthony Trollope's *Doctor Thorne*).

74. *See supra* Section I.A; *infra* Section VI.A.

The availability requirement is unusually challenging for election systems because (1) the group of people intended to access the system (i.e., the electorate) is highly diverse, and (2) concurrent confidentiality and integrity requirements in elections mean that ensuring secrecy and independence for every individual voter is paramount. An election system must allow all voters—regardless of education, technological proficiency, disability, or other characteristic—to cast a secret ballot, durably recorded with just as credible a guarantee of being correctly counted in the election outcome as any other voter's ballot.

Counting. A similar analysis of the *counting* guarantee yields additional requirements for election security. For example, the counting process must ensure that the preferences indicated on cast ballots are aggregated accurately (*integrity*), and the counting infrastructure must remain functional throughout the election (*availability*).

Checking. Finally, in case any of the preceding casting and counting requirements fail, the checking guarantee requires a publicly verifiable indication of failure. For example, if some ballots are lost or altered—due to human error, natural disaster, adversarial attack, or something else—the system must indicate the loss. This enables correction if adequate evidence is available or, in the worst case, allows for the election to be rerun—an undesirable eventuality that is nevertheless preferable to (perhaps unknowingly) accepting an incorrect outcome. For computer-based systems, this means ensuring that any computerized processes "show their work" in independently human-checkable form, thus providing evidence of their correct functioning (or evidence of any problems that occurred)[75]—a principle termed "software independence" in the election security literature in computer science.[76] The idea is that "you never want to be in a position where you have to say, '[The result is right just] because the computer says so!'"[77]

---

75. *See, e.g.*, JONES & SIMONS, *supra* note 3, at 93 (discussing a 2006 election in Sarasota County, Florida, where the voting machines produced no evidence trail so there was no way to investigate a significant statistical anomaly discovered after the election).

76. Ronald L. Rivest, *On the Notion of 'Software Independence' in Voting Systems*, 366 PHIL. TRANSACTIONS ROYAL SOC'Y 3759 (2008).

77. *Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House: Hearing Before the H. Comm. on House Admin.*, 116th Cong. (2020) (statement of Ronald L. Rivest, MIT Institute Professor); *see also In re* Voting

As described by CISA, "[e]very state has voting system safeguards to ensure each ballot cast in the election can be correctly counted" (*casting*) as well as "laws and processes to verify vote tallies before results are officially certified" (*counting*), including "robust chain-of-custody procedures, auditable logs, and canvass processes."[78] Furthermore, the use of paper records "allow[s] for tabulation audits [(i.e., checking tabulated values by inspecting the original voter-verified paper ballots)] to be conducted from the paper record in the event any issues emerge" (*checking*).[79] Finally, most stages of the election process (except, of course, the marking of the secret ballot by voters) are subject to observation—by bipartisan representatives, nonprofits, NGOs, and the public—as a transparency measure "to add an additional layer of verification."[80]

* * *

Current systems do not achieve perfection on casting, counting, or checking. Designing a perfect system is out of the reach of current human knowledge and will likely remain out of reach for the foreseeable future due to human fallibility.[81] How well, then, must each of the guarantees described above be satisfied? The kind of assurance considered adequate to support election outcomes as legitimate—as evidenced by broad acceptance, even if reluctantly, of the outcome across a given society—has changed over time, depending on societal context and norms as well as what is within the reach of contemporary system design. Such changes consistently intend to shift toward *stronger* security guarantees. Available alternatives are significant; a system that might once have been adequate may no longer be considered acceptable once a practical alternative with superior security guarantees is established. Next, I provide

Machine, 36 A. 716 (R.I. 1897) (Rogers, J., dissenting) (expressing a similar security requirement for voting machines over a century earlier).

78. *Rumor Control*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Nov. 8, 2022), https://www.cisa.gov/rumorcontrol [https://perma.cc/Z733-WBFP].

79. *Id.*

80. *Id.*; *see also* CARTER CTR., A GUIDE TO ELECTION OBSERVER POLICIES IN THE UNITED STATES (2016); S.W.L., *What Do Election Observers Do?*, ECONOMIST (June 21, 2017), https://www.economist.com/the-economist-explains/2017/06/21/what-do-election-observers-do [https://perma.cc/AH64-CXMH].

81. *See* sources cited *supra* note 54.

two illustrations of the evolution of societal expectations about secure election conduct in rather different contexts.

The history of the secret ballot provides one informative illustration. "For the first 50 years of American elections, . . . those with the right to vote (only white men at the time) went to the local courthouse and publicly cast their vote out loud" after "swear[ing] on a Bible that they were who they said they were and that they hadn't already voted."[82] The difference between then and now illustrates the extent of norm shifts over the centuries as well as the fallacy of opposing measures to strengthen election security on the grounds that the current system seems to function passably—a rationale as valid then as now. Paper ballots were first used in the nineteenth century, and government-printed, anonymous paper ballots (pioneered by the Australians in 1858) were first adopted in the late 1800s. Voting machines became popular in the United States from the early 1900s: first, mechanical lever machines, then punch cards and optical-scan technology, then touchscreen and other DRE voting machines, and most recently a shift back toward machines that (unlike lever or DRE machines) produce voter-verifiable paper records. Each of these transitions in voting technology were accompanied by concerns about the preceding technologies' reliability and the promise—whether or not borne out—that the new technology would improve election integrity.

The history of Black suffrage in the United States provides another illustration. Even after Black Americans' right to vote gained constitutional protection in the Fifteenth Amendment,[83] many serious barriers to access remained. Many eligible voters still did not have a meaningful opportunity to vote due to hostilities ranging from disguised and state-sponsored tactics, such as literacy tests, to overt but less official tactics, such as threats, violence, murders, and other forms of intimidation at the polls.[84] Over time and after much advocacy, many such

82. Dave Roos, *How Americans Have Voted Through History: From Voices to Screens*, HISTORY, https://www.history.com/news/voting-elections-ballots-electronic [https://perma.cc/N6TZ-WDVL] (Nov. 2, 2020); Douglas W. Jones, *A Brief Illustrated History of Voting* (2003), http://homepage.cs.uiowa.edu/~dwjones/voting/pictures [https://perma.cc/GQ27-S4Z9].

83. U.S. CONST. amend. XV.

84. *See* Brad Epperly et al., *Rule by Violence, Rule by Law: The Evolution of Voter Suppression and Lynching in the U.S. South* (2016) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3224412 [https://perma.cc/E9SB-8HP9]; V.O. KEY, JR., SOUTHERN POLITICS IN STATE AND

barriers became more widely recognized by judges and legislators as racially discriminatory and unacceptable, and new constitutional jurisprudence as well as legislation (e.g., the Voting Rights Act) were developed to improve the security of elections against such access barriers with varying success.[85] While the situation has improved enormously since the Fifteenth Amendment's passage, voter suppression persists today, and the process of improving access to elections for all eligible voters is an ongoing one, with growing public attention and better data about access barriers driving modern concerns and proposals for improvement.[86]

C. Security Properties of Traditional Paper-Ballot-Based Systems

Let us consider an old-fashioned paper-ballot-based election system with ballot secrecy, say, circa 1900. Traditional paper-ballot-based election systems provide remarkably robust support for the casting, counting, and checking guarantees in several respects—perhaps surprisingly, so much so that the state of the art in digital paperless technology is still unable to provide comparable guarantees in these respects.[87]

What, then, are the key security properties of an old-fashioned paper-ballot-based voting system? Voters can straightforwardly verify that the contents of their ballot match

---

NATION 555–618 (1949); Lassiter v. Northampton Bd. of Elections, 360 U.S. 45 (1959).

85. *See generally* Epperly et al., *supra* note 84.

86. *See* Lisa Marshall Manheim & Elizabeth G. Porter, *The Elephant in the Room: Intentional Voter Suppression*, 2018 SUP. CT. REV. 213 (2019); Zoltan Hajnal et al., *Voter Identification Laws and the Suppression of Minority Votes*, 79 J. POL. 363 (2017); Sarina Vij, *Why Minority Voters Have a Lower Voter Turnout: An Analysis of Current Restrictions*, 45 ABA HUM. RTS. MAG. (June 25, 2020), https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/voting-in-2020/why-minority-voters-have-a-lower-voter-turnout [https://perma.cc/D63F-WP69]; Danyelle Solomon et al., *Systemic Inequality and American Democracy*, CTR. FOR AM. PROGRESS (Aug. 7, 2019), https://www.americanprogress.org/article/systematic-inequality-american-democracy [https://perma.cc/AX7P-DRU4].

87. *See* NAS REPORT, *supra* note 2, at 6–7, 42; Appel & Stark, *supra* note 11; Park et al., *supra* note 72; *Paper Records*, VERIFIED VOTING, https://verifiedvoting.org/paperrecords [https://perma.cc/U5HE-HX2T]; Raj Karan Gambhir & Jack Karsten, *Why Paper Is Considered State-of-the-Art Voting Technology*, BROOKINGS (Aug. 14, 2019), https://www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology [https://perma.cc/NV2K-QDB4].

their intentions, at the time of casting, if they mark them by hand and then drop them in a box. Individual physical voting booths help ensure secrecy at the time of ballot marking, in a manner unparalleled by any remote voting method.[88] Tampering with ballots after they have been cast is difficult to achieve undetected if the ballot box is under continuous supervision and observation for the duration of the election. Tampering with paper ballots at scale is even more difficult, requiring human labor and risk of detection roughly in proportion to the number of ballots tampered.[89] Hand counting of paper ballots can be protected against human error as well as malice by having teams of multiple people count each ballot. Hand or machine counting of paper ballots can be protected against error and malice by post-election audits that cross-reference hand-inspected paper ballots. And, as CISA emphasizes, in case of any problem or dispute, there is an authoritative record of durable paper ballots to go back to and to recount if necessary.

However, paper ballots hand-marked in the traditional way have significant accessibility limitations, failing to provide a meaningful opportunity to vote to certain groups of eligible voters. Traditional hand marking of paper ballots is simply not a possibility for many voters with disabilities, as well as illiterate voters.[90] The groups that would be rendered unable to vote unassisted (and thus denied a secret ballot) by requiring hand-marked paper ballots make up a significant percentage of the United States population—currently available statistics do

88. Mail voting also suffers from less secrecy than in-person voting. However, mail voting is still robust in most of the other ways described in this paragraph, unlike non-paper-based remote voting methods. Where the choice is between remote voting or practically not being able to vote at all (e.g., overseas military, or citizens who reside overseas or have mobility constraints), mail voting is thus a preferred solution; where in-person voting is feasible, it is preferable to mail voting. *See* NAS REPORT, *supra* note 2, at 65–69; Park et al., *supra* note 72, at 6.

89. There are exceptions. For example, one could destroy many ballots at once by setting the ballot box on fire. But it would be essentially certain that such an attack would be detected. *See* NAS REPORT, *supra* note 2, at 43 (discussing the limitations of paper ballots).

90. *See* Am. Ass'n of People with Disabilities v. Hood, 278 F. Supp. 2d 1345 (M.D. Fla. 2003) (challenging paper-based voting systems on behalf of visually and manually impaired voters); *Voting, Accessibility, and the Law*, NAT'L FED'N OF THE BLIND, https://nfb.org/programs-services/center-excellence-nonvisual-access/national-center-nonvisual-election-3 [https://perma.cc/P6DV-MGRR] [hereinafter *NFB on Voting*]; *Making Their Mark*, ECONOMIST (Apr. 5, 2014), https://www.economist.com/international/2014/04/05/making-their-mark [https://perma.cc/7SUZ-P35N].

not yield a precise number, but it is at least 4 percent, and likely larger.[91] In many non-election-related situations, the accessibility of a service can be augmented by adding an *alternative* accessible way of using the service, but such solutions are often unsuitable for the election context; they are likely to violate important security guarantees (the secret ballot) and federal laws about accessibility[92] as well as undermine the independence and dignity of voters with disabilities. While important progress has been made in accessible voting system design in recent decades, building voting systems that provide commensurate integrity and verifiability guarantees to those offered by paper-based systems as described above—but for all eligible voters, including those who cannot hand mark paper ballots—remains a pressing and challenging question in election security.[93]

For our purposes, a traditional paper-ballot-based system provides an informative case study given that more than a century of history has established the security guarantees of a paper-based secret ballot as a baseline to improve upon. Today's election systems should provide at least comparable or better security guarantees to be considered adequate.

D. Benefits and Security Risks of Modern Technologies in Election Systems

Modern technology can and does play a role in many parts of today's election systems. The introduction of new technology has led to many significant improvements in security over the

91. *Disability Impacts All of Us*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/ncbddd/disabilityandhealth/documents/disabilities_impacts_all_of_us.pdf [https://perma.cc/G8UF-EHXF] (stating that 4.6 percent of adults in the United States are blind or have serious difficulty seeing and also stating larger percentages for disabilities related to mobility and cognition); U.S. DEP'T OF EDUC., ADULT LITERACY IN THE UNITED STATES 1 (2019), https://nces.ed.gov/pubs2019/2019179.pdf [https://perma.cc/BD3H-S78K] (stating that 4.1 percent of United States adults between ages sixteen and sixty-five are functionally illiterate in English and noting that the largest low-literacy groups by nativity and ethnicity are United States born and White). I was not able to find data on the size of these groups together or on the fraction of those functionally illiterate in English who read another language, and I was not able to find data on the fraction of people described as having disabilities related to mobility or cognition who would find it difficult to vote by hand-marked paper ballot.

92. Americans with Disabilities Act (ADA) of 1990, 42 U.S.C. §§ 12101–12213 (2000); HAVA, 52 U.S.C. §§ 20901–21145 (2023).

93. *See* NAS REPORT, *supra* note 2, at 79–80.

years, for example, in voter registration, results reporting, and accessibility.

Statewide electronic voter registration databases and electronic pollbooks have greatly streamlined the efficiency and reliability of managing voter registration information. Digitally cross-checking voter registration information against other electronic databases—such as driver registration records, post office records, and other state voter databases—has also improved the accuracy and timely update of voter information.[94] Of course, security is critical in managing voter registration information; while modern registration systems following security best practices have great benefits, multiple poorly secured voter databases have suffered attacks,[95] underscoring the need for security expertise and training for all election infrastructure.

Technology has also long played a key role in streamlining election results reporting ever since the telegraph's first use in 1848 to quickly transmit vote counts from coast to coast, a massive improvement from relying on transmission of results "from distant precincts on horseback, carriage, or train."[96] Today, radio, television, and the internet have further transformed the way election night reporting is done. Security in results reporting is essential too; the EAC has issued guidance on recommended security practices.[97] State *certification* of

94. *E.g.*, *ERIC at Work*, ELEC. REGISTRATION INFO. CTR. (2018), https://ericstates.org/statistics [https://perma.cc/K6PC-XKCS].

95. *See* NAS REPORT, *supra* note 2, at 26–27, 58; Catalin Cimpanu, *US Voter Records from 19 States Sold on Hacking Forum*, ZDNET (Oct. 15, 2018), https://www.zdnet.com/article/us-voter-records-from-19-states-sold-on-hacking-forum [https://perma.cc/6X9P-X9NX]; *Illinois Elections Board Offers More Information on Hacking Incident*, ILL. PUB. RADIO (May 4, 2017), https://news.wsiu.org/politics-elections/2017-05-04/illinois-elections-board-offers-more-information-on-hacking-incident [https://perma.cc/BGP3-EXY7]; Katie Reilly, *Russians Hacked Arizona Voter Registration Database*, TIME (Aug. 30, 2016), http://time.com/4472169/russian-hackers-arizona-voter-registration [https://perma.cc/SW38-D8HW]; Frank Bajak, *Georgia Election Server Wiped After Suit Filed*, AP NEWS (Oct. 26, 2017), https://www.apnews.com/877ee1015f1c43f1965f63538b035d3f [https://perma.cc/52L8-VV36]; MUELLER REPORT, *supra* note 42, at 50.

96. Rebecca Onion, *When Did We Start to Expect Results on Election Night?*, SLATE (Nov. 3, 2020), https://slate.com/news-and-politics/2020/11/election-night-results-expectation-history.html [https://perma.cc/8HUR-EC7M].

97. *Checklist for Securing Election Night Reporting Systems*, U.S. ELECTION ASSISTANCE COMM'N (Oct. 23, 2017), https://www.eac.gov/documents/2017/10/23/checklist-for-securing-election-night-reporting-systems-data-election-administration-security [https://perma.cc/P2HQ-TNFX].

official election results (following media reporting of unofficial election results) is yet another step with separate requirements to reporting.[98]

Accessibility is a third area where modern technology has opened new possibilities. Voters unable to use traditional paper ballots used to be required to compromise their independence and ballot secrecy by asking another person to fill out and cast their ballot for them—and hoping that their instructions would be faithfully followed.[99] In recent decades, new technologies have enabled some of these voters to independently cast secret ballots, although much progress remains to be made.[100] Such technologies gained prominence after 2002 due to HAVA's accessibility provisions.[101] Some of these technologies entirely replace voter-verifiable paper records with unverifiable alternatives. Unfortunately, research since HAVA has established that such approaches entail serious security flaws.[102] However, other technologies for accessible vote casting, such as ballot-marking devices—that is, devices that allow a voter to mark a paper record whose contents the voter can verify before casting—show promise in improving accessibility while also preserving more of the strong security properties of traditional paper-based systems.[103] Furthermore, such new technologies may provide usability benefits for all voters,[104] for example by flagging possible mistakes such as not marking any candidate for president.[105]

* * *

98. *See* Patrick Howell O'Neill, *How Election Results Get Certified*, MIT TECH. REV. (Nov. 17, 2020), https://www.technologyreview.com/2020/11/17/1012203/how-election-results-get-certified [https://perma.cc/AW9C-6CX2].

99. *See* NOEL H. RUNYAN, IMPROVING ACCESS TO VOTING: A REPORT ON THE TECHNOLOGY FOR ACCESSIBLE VOTING SYSTEMS 8 (2007).

100. *See id.*

101. *Id.*

102. *Id.* at 8–9.

103. *See* NAS REPORT, *supra* note 2, at 39, 42, 76. *But see* Andrew Appel et al., *Ballot-Marking Devices Cannot Assure the Will of the Voters*, 19 ELECTION L.J. 432 (2020) (arguing that currently available ballot-marking device technologies are not secure enough for widespread use).

104. Elizabeth F. Emens, *Integrating Accommodation*, 156 U. PA. L. REV. 839, 845–65 (2008).

105. Paul M. Schwartz, *Voting Technology and Democracy*, 77 N.Y.U. L. REV. 625, at 631, 696 (2002) (describing feedback to voters about potential mistakes in filling out a ballot as a "critical technological advantage" and recommending adoption of voting techniques that facilitate such feedback).

It may seem remarkable that the state of the art in modern technology does not provide techniques to achieve similarly strong integrity and verifiability guarantees when replacing paper-ballot-based systems with technology that does not create a voter-verifiable paper evidence trail. Part of the challenge is that modern technology is often susceptible to hard-to-detect attacks that can be executed remotely. More complexity can actually be a drawback here, as it makes detection harder and presents more opportunities for attacks, especially at a large scale. Another part of the challenge is more basic: modern software engineering has not figured out how to build computer systems free of "bugs" or errors.[106] While we are able to build remarkably complex, apparently functioning computer-based systems, they are constantly tweaked and refined to remove bugs as they are discovered in a process that is always ongoing and never considered complete.[107] Seemingly security-critical systems such as electronic banking actually *often fail*, in ways that are hidden behind the scenes, and are designed in the anticipation of paying the costs of failure in monetary terms (e.g., through insurance).[108] Of course, insurance cannot provide a solution for election insecurity; the requirements of a democratic election cannot be satisfied by simply paying off the people whose votes were not counted.

Concretely, let us contrast with the security properties of paper ballots as discussed in Sections II.C and II.E. Individual physical voting booths provide a much weaker guarantee of secrecy if the voter is using technology that might, if wrongly configured or compromised, be accessible from outside the booth or store cast votes with identifying information. Voters cannot verify the contents of an electronic ballot at the time of casting as it is not practicable for them to inspect the actual electronic

106. Appel & Stark, *supra* note 11, at 524 n.1 ("The vulnerability of computers to hacking is well understood. Modern computer systems, including voting machines, have many layers of software, comprising millions of lines of computer code; there are thousands of bugs in that code . . . . A software-based product such as a voting machine can be expected to contain, at any given time, one or more exploitable security vulnerabilities."); *see also* sources cited *supra* note 54.

107. *See supra* note 106.

108. *See* JONES & SIMONS, *supra* note 3, at 273 (quoting Harri Hursti, in the context of selling online banking software, as saying, "Our sales point was always, 'Yes, we will introduce more fraud. However, we will introduce cost savings which will greatly offset the increased amount of fraud.'"); Park et al., *supra* note 72, at 2; JOSEPHINE WOLFF, CYBERINSURANCE POLICY: RETHINKING RISK IN AN AGE OF RANSOMWARE, COMPUTER FRAUD, DATA BREACHES, AND CYBERATTACKS 1–3 (2022).

information being saved or transmitted out of the voting machine—and any human-readable representation of the ballot they see might not match with the actual information being electronically transmitted if the machine is wrongly configured or compromised.[109] Undetected tampering with electronic ballots after they have been cast may be possible if the ballot storage equipment is wrongly configured or compromised, and continuous observation of the equipment is unlikely to be able to detect sophisticated attacks. Tampering with electronic ballots *at scale* is often as little effort as tampering with just a few ballots, if the storage equipment is wrongly configured or compromised. Consider, for example, that editing a single cell in a spreadsheet is as quick as editing a whole column at once. The risk of detection for someone attempting ballot tampering can also be much lower due to the preceding factors, among others. Hand inspection or counting of purely electronic ballots is not practicable, as noted above. Thus, machine counting of paper ballots cannot be verified by post-election audits that cross-reference hand-inspected ballots. In case of a problem or dispute, the only record to go back to is electronic, a form that is not directly human-readable and is much more susceptible to tampering than paper-based alternatives.

These types of security weaknesses are exactly those underlying many of the vulnerabilities discovered and demonstrated in security researchers' reports over the years.[110] Many of the egregious examples from those reports—for example, paperless voting machines that allow tampering by anyone with sufficient know-how who has physical access to the machine for a few minutes[111]—can be considered neither to provide a meaningful opportunity to cast a vote (*casting*), nor to provide a strong guarantee that the reported election outcome is consistent with the votes actually cast (*counting*), nor to provide credible public assurance of a correct outcome by ensuring detection of errors (*checking*).

109. *See also* NAS REPORT, *supra* note 2, at 94.

110. *See* sources cited *supra* note 3.

111. *E.g.*, Ed Felten, *Report Claims Very Serious Diebold Voting Machine Flaws*, FREEDOM TO TINKER (May 11, 2006), https://freedom-to-tinker.com/2006/05/11/report-claims-very-serious-diebold-voting-machine-flaws [https://perma.cc/9JZM-FPWM].

E. How Paper Ballots Can Enhance the Security of a Machine Count

In the United States today, even where paper ballots are used, tallying is performed by machine, except in special circumstances calling for a hand recount.[112] Sometimes tallying is done by scanning ballots and then processing the output of the scan (e.g., digital ballot images) using tabulation software that interprets the scan output and tallies the interpreted results. Sometimes—in the so-called "DRE with VVPAT" model[113]—tallying is performed electronically by DRE voting machines based on information stored electronically in the machines when voters use them to vote; but there is still a human-readable paper ballot. The paper ballots are printed when the voter is ready to cast their vote on the machine. The paper should reflect the voter's electronic (e.g., touchscreen) selections, and the voter can and should review the paper before the final act of casting.

How can paper ballots provide additional security if the tallying is done by machine and the election outcome is determined from the machine tally? This is a natural question—and indeed, misinterpretations of paper ballots' security properties have led some to claim that the paper's purpose is just to "comfort" voters.[114] Such claims are false. In fact, paper ballots provide a strong guarantee of the correctness of an election outcome based on a machine tally when accompanied by post-election audits. Remarkably, such audits generally need not manually examine all or nearly all ballots to achieve high confidence.

Post-election audits may use various approaches to check whether an election was conducted properly.[115] Some traditional kinds of post-election audits have been routinely performed and legally required for decades.[116] A newer type of audit, called a

112. *See supra* Section II.A.

113. Originally, DRE machines did not produce paper records. The addition of printers was a result of later reform due to security concerns. VVPAT stands for "voter-verifiable paper audit trail." *See* sources cited *supra* note 31.

114. Dan Goodin, *US Expat Casts Ballot from Vienna, Wonders If Anyone Got It*, REGISTER (Feb. 6, 2008), https://www.theregister.com/2008/02/06/expat_voting_system_questions [https://perma.cc/28HK-62A2].

115. *See* NAS REPORT, *supra* note 2, at 53, 93–96; Mark Lindeman & Philip B. Stark, *A Gentle Introduction to Risk-Limiting Audits*, 10 IEEE SEC. & PRIVACY 42 (2012).

116. NAS REPORT, *supra* note 2, at 94.

risk-limiting audit (RLA), offers a statistical check on the correctness of a reported election outcome far more efficiently than previous methods.[117] RLAs work by manually reexamining some ballots in order to confirm that the votes observed are statistically consistent with the reported election outcome.[118] An RLA differs from a manual recount in that the RLA aims to corroborate the reported election outcome while manually examining just a small sample of ballots, far fewer than all ballots cast. However, if the initial steps of an RLA reveal a potential inconsistency, it may be necessary to examine more ballots or do a full recount in order to confirm the reported election outcome.[119] Crucially, RLAs "can efficiently establish high confidence in the correctness of election outcomes—even if the equipment used to cast, collect, and tabulate ballots to produce the initial reported outcome is faulty."[120]

That said, even absent post-election audits, paper ballots provide a smaller but still significant security benefit over paperless systems: they provide a voter-verified record to reference in case of a dispute or recount request. Without paper records, no meaningful recount is possible; the machine will "simply spit out the same tally as before."[121]

Paper ballots provide security benefits *only if used correctly*, however. The voter must have the opportunity to inspect the record and to rectify it before casting the ballot in case it contains errors (i.e., votes different from the voter's intent)[122]—otherwise, a machine could simply print out a record consistent with its reported tally, regardless of voters' intent. Moreover, paper ballots only provide a strong guarantee of correctness in conjunction with routine post-election audits. The paper ballots

117. *Id.*

118. *Id.*

119. *Id.*

120. *Id.* at 100. An RLA would establish such confidence in the initial reported outcome only if that reported outcome was correct despite the faultiness of the equipment. Otherwise, if there were an error in the reported outcome, the RLA would flag the error, thus facilitating correction of the results by recounting. In either case, the use of an RLA establishes high confidence in the ultimate outcome—whether it be the initial reported outcome or a corrected one.

121. John Ensign, *How to Make Sure That Your Vote Counts*, N.Y. TIMES (Dec. 15, 2003), https://www.nytimes.com/2003/12/15/opinion/how-to-make-sure-that-your-vote-counts-4-letters.html [https://perma.cc/ZC93-H3GF].

122. Hand-marked ballots are even better in this regard since the necessary act of marking ensures that the ballot is voter *verified*, not just voter *verifiable*. But accessibility does not always permit hand marking of ballots, and then, voter-verifiable, machine-marked ballots are a good alternative.

can only reveal errors in the election outcome if they are checked against the tally—and without post-election audits, that would likely only happen in case of a dispute or recount, instead of routinely after each election. If the paper is never referenced, then it will not have any effect.

In summary, paper ballots can offer greatly enhanced security to machine-tallied elections by strengthening the *checking* guarantee. The move from paperless electronic machines to paper-ballot or VVPAT-based voting systems in most states, and the increase in the quality and frequency of post-election auditing in many states, have been the key features of the improvement in election system security over the last decade and a half.

F. Potential Risk, Realized Risk, and Magnitude of Risk (or Vulnerabilities and Exploitation)

It is important to distinguish the concepts of potential risk, realized risk, and magnitude of risk arising from security weaknesses in systems.

When someone discovers and describes a security weakness, they have documented the existence of a *potential* risk to the system. In the security community, this is called a *vulnerability*. If someone takes their knowledge of a vulnerability and uses it to damage the confidentiality, integrity, or availability of a nonexperimental system, they have *realized* that potential risk. In the security community, this is called *exploitation*; a specific method for exploiting the vulnerability is called an *exploit*.

Confusingly, the term *attack* can be used to describe either vulnerabilities or exploits. A vulnerability is essentially the description of an attack; an exploit is the attack executed on a real system.

Understanding and disseminating information about vulnerabilities is considered an essential part of building secure systems. Since systems are imperfect, we strive to learn about their vulnerabilities in order to understand how to mitigate them and thus better secure the systems in future[123] (however,

123. *See Cyber-Threat Intelligence Information Sharing Guide*, U.K. NAT'L CYBER SEC. CTR. (Mar. 8, 2021), https://www.gov.uk/government/publications/cyber-threat-intelligence-information-sharing/cyber-threat-intelligence-information-sharing-guide [https://perma.cc/CH8E-FTP4]; *Known Exploited Vulnerabilities Catalog*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/known-

deliberate exploitation is *not* a standard part of the research or development process). A preemptive approach to systems security is critical for building resilient systems, given that exploits can be unexpected and hard to detect and can cause ongoing surreptitious damage until a mitigation is deployed[124]—a point of importance for Part IV's legal theory, which promotes preemptive redress.

The likelihood that a vulnerability will be exploited—that is, that a potential security risk will be realized—depends on many factors.[125] Technical factors include the nature of specialized knowledge, equipment, network access; credentials required to perform the corresponding exploit; and what kinds of hardware and software are susceptible. Essentially, a technical analysis examines *how hard it would be* to perform the exploit. But the *likelihood*, or precise magnitude of risk, that a vulnerability will be exploited depends on many additional nontechnical factors: economic, sociological, anthropological, political, and more.[126] As such, any quantification of the likelihood of exploitation will inherently contain far larger uncertainty than a purely technical analysis of a vulnerability's severity.

In the computer security community, methods of assessing and describing the severity of vulnerabilities often focus on the technical question of how difficult exploitation would be.[127] Often, vulnerability research provides only a technical analysis of severity, without reaching nontechnical factors or probability of exploitation (and rightly so, where the researcher's expertise

exploited-vulnerabilities-catalog [https://perma.cc/F4QT-PFU8]; *Security Vulnerabilities*, CARNEGIE MELLON UNIV. SOFTWARE ENG'G INST., https://www.sei.cmu.edu/our-work/security-vulnerabilities [https://perma.cc/8H2Y-3YBB].

124. *See generally* Ron Ross et al., *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, 2 NIST SPEC. PUB. 800-160, Nov. 2021.

125. *See* GREGORY ALLEN & RACHEL DERR, THREAT ASSESSMENT AND RISK ANALYSIS: AN APPLIED APPROACH 97–106 (2016).

126. For example, what is at stake? Who is incentivized to perform exploitation? What resources and expertise are they likely to have? What weaknesses are they likely to have? What would be the social, political, economic, or other consequences of the exploitation being publicized? And so on. *See id.*

127. *See generally* ADAM SHOSTACK, THREAT MODELING: DESIGNING FOR SECURITY (2014); JACKSON WYNN ET AL., MITRE, THREAT ASSESSMENT & REMEDIATION ANALYSIS (TARA) 32–34 (2011), https://www.mitre.org/sites/default/files/2021-10/pr-14-2359-tara-introduction-and-overview.pdf [https://perma.cc/BC9K-DM4Y]; *Vulnerability Metrics*, NAT'L INST. OF STANDARDS & TECH., https://nvd.nist.gov/vuln-metrics [https://perma.cc/8Z7H-79ZL].

is only technical). Especially for severe vulnerabilities in high-stakes situations, mitigation efforts may proceed immediately based on such technical analysis, without (or before) estimating the precise likelihood of exploitation.

* * *

Vulnerabilities and exploits appear closely related. As such, the concepts are sometimes conflated in popular perception. A prominent and unfortunate recent example comes from Trump and some of his supporters' claims that the 2020 election was "stolen" and involved "massive fraud," where they cited reputable security research in supposed support of their allegations.[128] Security researchers were swift to rebut and underscore the difference between potential and realized risk:

> The presence of security weaknesses in election infrastructure does not by itself tell us that any election has actually been compromised. Technical, physical, and procedural safeguards complicate the task of maliciously exploiting election systems, as does monitoring of likely adversaries by law enforcement and the intelligence community. Altering an election outcome involves more than simply the existence of a technical vulnerability.[129]

In other words, the reference to reputable security research to support such fraud claims is like citing reputable research showing that a certain kind of front door lock can be picked with a hairpin (i.e., a vulnerability) to prove an allegation that millions of houses in carefully guarded gated communities were broken into by lockpicking last year, and millions of valuables were stolen (i.e., exploitation at a massive scale). The causality is just not there, even if many of the houses in question used those faulty locks. Of course, that does not mean there is no need to fix the locks. The flaws in the locks are real, they pose a real threat to safety, and they should be fixed as soon as possible. At the same time, claims of massive break-ins and theft are not credible absent specific evidence of the same. They are all the less credible in a context with extensive procedural security measures beyond the flawed technology itself, such as security

128. *See* Trump, *supra* note 7.
129. Adams et al., *supra* note 49.

guards and surveillance cameras in the case of a housing complex or chain-of-custody monitoring and post-election auditing in the case of elections.

III. LEGAL BACKGROUND

This Part reviews the law potentially applicable to securing election infrastructure and election administration. Election management in the United States is highly decentralized: local officials bear most of the responsibility for conducting elections, so large variations in election systems can occur even within a single state.[130] Federal involvement in election administration is limited, and most decisions are made at the state or local levels.

Next, Section III.A describes relevant constitutional doctrines, and Section III.B discusses statutory requirements on election administration.

A. The Constitutional Right to Vote

The U.S. Constitution does not explicitly enumerate a right to vote, but instead implies the existence of such a right through its amendments prohibiting abridgment of that right on the basis of race,[131] sex,[132] or payment of a poll tax[133] for anyone over eighteen years of age.[134] The Supreme Court has "repeatedly recognized that all qualified voters have a constitutionally protected right to vote, and to have their votes counted,"[135] and has long described the right to vote as "fundamental" and "preservative of all rights."[136]

Moreover, "the right to vote is the right to participate in an electoral process that is necessarily structured to maintain the integrity of the democratic system."[137] Other dicta in Supreme Court voting rights cases reinforce this perspective, for example, by emphasizing the importance of "public confidence in the

130. LOWENSTEIN ET AL., *supra* note 7373, at 375.
131. U.S. CONST. amend. XV.
132. U.S. CONST. amend. XIX.
133. U.S. CONST. amend. XXIV.
134. U.S. CONST. amend. XXVI.
135. Reynolds v. Sims, 377 U.S. 533, 554 (1964) (citation omitted).
136. Yick Wo v. Hopkins, 118 U.S. 356, 370 (1886); Ill. State Bd. of Elections v. Socialist Workers Party, 440 U.S. 173, 184 (1979); *see, e.g.*, *Reynolds*, 377 U.S. at 562.
137. Burdick v. Takushi, 504 U.S. 428, 441 (1991).

integrity of the electoral process" for "citizen participation in the democratic process."[138] Effectively, "the right to vote"—both legally and colloquially—is shorthand for all of the above requirements combined.[139]

There are at least three[140] federal constitutional voting rights doctrines that bear on election security under which a constitutional right to vote *securely* might naturally arise: (1) the *Anderson-Burdick* balancing test for burdens on the right to vote, (2) *Bush v. Gore*'s prohibition of arbitrary and disparate treatment of voters, and (3) vote dilution. State constitutional voting rights may afford additional protection.

Anderson-Burdick*: Burdens on the right to vote.* Government-imposed burdens on voting rights are unconstitutional under the First and Fourteenth Amendments unless they are adequately justified as furthering an important state interest.[141] *Anderson* and *Burdick* involved constitutional challenges to an early filing deadline for independent candidates and a ban on write-in voting, respectively.[142] The Supreme Court deemed the deadline in *Anderson* to be a severe burden on voting and associational rights[143] and held it

138. Crawford v. Marion Cnty. Election Bd., 553 U.S. 181, 197 (2008).

139. Another possible interpretation is that the requirement of correct counting and reporting is implicit in the right to cast a vote because the concept of "casting" a vote entails not only the idea that the ballot leaves the voter's hands and is submitted to the election system but also that the election system is one that will subsequently reliably count and report it. This seems a reasonable interpretation of the term "cast a vote." However, in this Article, the term "casting" is used to mean an act the voter performs that is intended to cause the submission of a ballot to the election system. This Article adopts this terminology both because it is helpful to distinguish the act of ballot submission from what happens to the ballot after submission, and because it is more consistent with the Supreme Court's language about ballot casting and subsequent counting and recording of ballots.

140. A fourth theory is that use of voting equipment that disproportionately negatively impacts minority votes may be a violation of section 2 of the Voting Rights Act. *See* Black v. McGuffage, 209 F. Supp. 2d 889, 894 (N.D. Ill. 2002); Common Cause S. Christian Leadership v. Jones, 213 F. Supp. 2d 1106, 1110 (C.D. Cal. 2001); Roberts v. Wamser, 679 F. Supp. 1513, 1531 (E.D. Mo. 1987); Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1743 (2005). I do not discuss such challenges in more detail. This Article aims to focus on legal responses to insecure election infrastructure as a general phenomenon rather than specific harms that may result from insecurity, and also, the strength of such Voting Rights Act claims has diminished considerably since the Supreme Court's narrow interpretation of section 2 in Brnovich v. Democratic Nat'l Comm., 141 S. Ct. 2321 (2021).

141. *See* Anderson v. Celebrezze, 460 U.S. 780 (1982); *Burdick*, 504 U.S. 428.

142. *Anderson*, 460 U.S. 780; *Burdick*, 504 U.S. 428.

143. The Article will henceforth use "voting rights" to include "associational rights" for brevity.

unconstitutional,[144] but considered the burden imposed by the ban in *Burdick* to be "slight" and "very limited" and upheld the ban.[145]

Under the *Anderson-Burdick* balancing test (sometimes characterized as a "sliding scale"),[146] the level of scrutiny to be applied to a challenge to an election regulation depends on the magnitude of the burden it places on voting rights.[147] Severe burdens call for strict scrutiny, while more limited burdens call for more permissive scrutiny.[148] Any burden, "however slight,"[149] is subject to *Anderson-Burdick* analysis, meaning that essentially any election regulation is properly treated as a burden.[150]

The Supreme Court more recently applied the *Anderson-Burdick* framework in *Crawford v. Marion County Election Board* to a law requiring photographic identification to vote. The opinions in *Crawford* indicated significant divergence in the Justices' views on the fact-specific application of the balancing test. Lower court decisions applying *Anderson-Burdick* in other contexts underscore its highly fact-dependent nature. For example, regulations requiring documentary proof of eligibility to vote were upheld and struck down in different contexts,[151] as were provisions limiting early voting opportunities, even by the same Court of Appeals.[152]

Bush v. Gore*: Arbitrary and disparate treatment of voters.* The highly publicized case of *Bush v. Gore* came in the aftermath of the closely contested presidential election of 2000. At issue were Florida rules for manually evaluating the intent of the voter on ballots not clearly enough marked to be machine-

144. *Anderson*, 460 U.S. at 783, 823.

145. *Burdick*, 504 U.S. at 437, 439.

146. *See* Crawford v. Marion Cnty. Election Bd., 553 U.S. 181, 210 (2008) (Souter, J., dissenting); Daunt v. Benson, 956 F.3d 396, 408 (6th Cir. 2020).

147. *Anderson*, 460 U.S. 780; *Burdick*, 504 U.S. 428.

148. *Burdick*, 504 U.S. at 434.

149. *Crawford*, 553 U.S. at 191.

150. *Burdick*, 504 U.S. at 433 ("Election laws will invariably impose some burden upon individual voters.").

151. *See Crawford*, 553 U.S. 181 (2008) (holding constitutional Indiana's requirement of government-issued photo identification to vote); Fish v. Schwab, 957 F.3d 1105 (10th Cir. 2020) (holding unconstitutional Kansas's requirement of documentary proof of citizenship to vote).

152. *See* Obama for Am. v. Husted (*Husted I*), 697 F.3d 423 (6th Cir. 2012) (holding likely unconstitutional Ohio's elimination of in-person early voting for nonmilitary voters); Ohio Democratic Party v. Husted (*Husted II*), 834 F.3d 620 (6th Cir. 2016) (holding constitutional Ohio's reduction of early voting days).

read.[153] The Court determined that "[t]he want of [specific rules designed to ensure uniform treatment] ha[d] led to the unequal evaluation of ballots in various respects," and further emphasizing that "[t]he formulation of uniform rules to determine intent" from ballot markings "is practicable," the Court held that such rules were constitutionally "necessary" and Florida's system was therefore unconstitutional.[154]

The Court held in *Bush v. Gore* that the Equal Protection Clause prohibits "arbitrary and disparate treatment" by a state toward "the members of its electorate," because "nonarbitrary treatment of voters [is] necessary to secure the fundamental right[to vote]."[155] This extended the Court's reasoning in *Gray v. Sanders*, which had decades earlier held unconstitutional a system that unequally weighted the votes of Georgia voters depending on where they lived.[156] More concretely, a state may not run an election system that, "by . . . arbitrary and disparate treatment, value[s] one person's vote over that of another" or imposes election procedures that cause an "unequal evaluation of ballots" cast by different voters.[157]

Election practices held unconstitutional under *Bush v. Gore*'s "arbitrary and disparate treatment" theory include:[158] disqualifying certain types of provisional ballots cast at the wrong location but not others;[159] offering disparate early voting opportunities for military and nonmilitary voters;[160] applying informal, subjective procedures to determine voters' eligibility to vote when challenged and treating challenges from different parties differently;[161] and deploying multiple voting

153. Bush v. Gore, 531 U.S. 98, 100–03 (2000).

154. *Id.* at 106.

155. *Id.* at 104–05.

156. 372 U.S. 368, 381 (1963).

157. *Bush*, 531 U.S. at 104–06.

158. The Supreme Court never subsequently cited *Bush v. Gore*, and the case itself suggests that it should not be used as precedent, but lower courts have applied it. *See* cases cited *infra* notes 159–162.

159. *See* Hunter v. Hamilton Cnty. Bd. of Elections, 635 F.3d 219 (6th Cir. 2011) (holding unconstitutional the disqualification of provisional ballots cast at the wrong subdivision within the correct polling location, while provisional ballots cast at the central office of the County Board of Elections, though cast in the wrong location, were not disqualified).

160. *See* Husted I, 697 F.3d 423 (6th Cir. 2012) (holding unconstitutional the provision of more early voting days for military than nonmilitary voters).

161. *See* Charfauros v. Bd. of Elections, 249 F.3d 941, 955 (9th Cir. 2001) (holding unconstitutional an election board's reliance on "the subjective testimony of one individual" to determine voter eligibility when challenged and its processing

technologies with different accuracy/error rates.[162] The most apposite precedent is *Stewart v. Blackwell*, in which the Sixth Circuit held unconstitutional Ohio's continued use of "antiquated voting equipment" well recognized as "inherently flawed" and likely to disenfranchise "thousands of Ohio voters" when used alongside more modern technology.[163]

Vote dilution. "Vote dilution" refers to diminishing the relative weight of certain voters' votes compared to others, without preventing them from casting ballots.[164] Election practices that cause vote dilution have been held to be unconstitutional in a number of contexts related to electoral districting: overpopulated districts dilute their residents' votes (relative to votes from less populated districts); the votes of minority voters who have been "packed" or "cracked" by strategically drawn district boundaries may be diluted; and similarly, partisan gerrymandering may cause dilution of the votes of a group with a particular political preference.[165] The constitutional problem arises when one person's vote is made to count for less than it ought to, since "the right of suffrage can be denied by a debasement or dilution of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise."[166]

---

of eligibility challenges raised by one political party before an upcoming election while delaying challenges raised by the other party until after).

162. *See* Stewart v. Blackwell, 444 F.3d 843 (6th Cir. 2006) (holding unconstitutional the use of multiple voting technologies with significantly differing accuracy/error rates); Sw. Voter Registration Educ. Project v. Shelley, 344 F.3d 882 (9th Cir. 2003) (finding likely success of a constitutional challenge to unreliable voting equipment at preliminary injunction stage); Wexler v. Anderson, 452 F.3d 1226 (11th Cir. 2006) (addressing a *Bush v. Gore* challenge to insecure election technology with an *Anderson-Burdick* analysis).

163. *Stewart*, 444 F.3d at 870.

164. *See, e.g.*, LOWENSTEIN ET AL., *supra* note 73, at 216.

165. *See, e.g.*, Reynolds v. Sims, 377 U.S. 533 (1964); White v. Regester, 412 U.S. 755 (1973); Davis v. Bandemer, 478 U.S. 109 (1986); Rucho v. Common Cause, 139 S. Ct. 2484 (overruling *Bandemer* and holding challenges to political gerrymandering to be non-justiciable). Other constitutional voting rights cases in other contexts often invoke the language of vote dilution in describing the right to vote. However, *Anderson-Burdick* and *Bush v. Gore* (i.e., arbitrary and disparate treatment) cases are doctrinally mostly distinct from the districting-based vote dilution cases and, as such, are not generally categorized as vote dilution cases by election law scholars. *See generally* LOWENSTEIN ET AL., *supra* note 73, at 141.

166. *Reynolds*, 377 U.S. at 555. Often, language about vote dilution focuses on one person's vote counting for less than another's—phrasing that is arguably a proxy for counting less than it ought to, since everyone's vote ought to count equally. I believe that if everyone's vote were equally discounted—to give an extreme

State constitutions. Unlike the federal constitution, almost all state constitutions contain explicit language granting the right to vote,[167] and most state constitutions also guarantee secrecy in voting.[168] "[T]he prevailing norm for most state constitutional adjudication"[169] in right-to-vote and related Equal Protection Clause cases is a lockstep approach in which state courts "simply follow[] federal jurisprudence for the analogous right," effectively "declaring that state law goes only as far as federal law."[170] Academic criticism has described the lockstep approach as "often [resulting in] a derogation of citizens' state constitutional right to vote" because state constitutions "go further than the U.S. Constitution in conferring voting rights."[171] A few state courts take a more state-focused approach in which courts "giv[e] independent force to state constitutional protections of individual liberties, such as the right to vote," subject to "the 'federal floor' of federal court jurisprudence [in cases where] the state constitution is insufficient."[172] Further details of state constitutional law are beyond the scope of this Article.

B. Statutory Constraints on Election Administration

Federal statutory requirements. Three federal statutes notably constrain state and local election administration: the Voting Rights Act (VRA), the National Voter Registration Act (NVRA), and HAVA. The VRA deals with features of election administration that could racially discriminate against certain voters.[173] The NVRA aims to promote voter registration by

example, flipping a coin to decide whether each vote should be counted—that would go just as much against equal protection as a classic vote dilution case.

167. *See* Joshua A. Douglas, *The Right to Vote Under State Constitutions*, 67 VAND. L. REV. 89, 144–49 (2019).

168. CAITRIONA FITZGERALD ET AL., THE SECRET BALLOT AT RISK: RECOMMENDATIONS FOR PROTECTING DEMOCRACY 6 (2016). States' detailed approaches to ballot secrecy vary considerably.

169. Douglas, *supra* note 167, at 106 n.104 (citing Michael E. Solimine, *Supreme Court Monitoring of State Courts in the Twenty-First Century*, 35 IND. L. REV. 335, 338 (2002) (explaining that "systematic studies demonstrate that most state courts, when presented with the opportunity, have chosen not to depart from federal precedents when interpreting the rights-granting provisions of state constitutions")).

170. Douglas, *supra* note 167, at 94, 105.

171. *Id.* at 110.

172. *Id.* at 111, 94.

173. LOWENSTEIN ET AL., *supra* note 73, at 424.

requiring states to support certain registration methods.[174] Insecure election infrastructure could conceivably facilitate violations of the VRA and the NVRA;[175] however, the statutes do not provide direct guidance on how to secure elections.

It is HAVA, "the federal government's most significant intervention to date in the 'nuts and bolts' of election administration,"[176] that bears most directly on election security.

In relevant part,[177] Title III of HAVA introduces certain requirements on states' administration of federal elections. Regarding election technology, Title III requires that marked ballots are verifiable by voters before casting (and can be corrected if errors are discovered);[178] that voting systems produce an auditable record of cast votes;[179] that there be at least one accessible voting machine for voters with disabilities "that provides the same opportunity for access and participation (including privacy and independence) as for other voters;"[180] and that the error rate of tabulation technology must comply with standards set by the Federal Election Commission.[181] Title III also requires states to make provisional voting available to voters whose registration or eligibility is contested at the polling place[182] and to maintain an authoritative "computerized statewide voter registration list" with "adequate technological security measures to prevent the unauthorized access" as well as provisions to ensure the list is accurate and up to date.[183]

Title I of HAVA authorizes federal funds for improving federal election administration, including the acquisition and upgrade of "voting systems and technology and methods for

174. *Id.* at 447.

175. For example, election technology that disproportionately negatively impacts minority voters arguably violates the VRA. *See supra* note 140 (discussing relevant case law).

176. LOWENSTEIN ET AL., *supra* note 73, at 450.

177. The details of Titles IV–IX of HAVA are not relevant to the present Article so I do not discuss them further.

178. HAVA, 52 U.S.C. § 21081(a)(1)(A).

179. 52 U.S.C. § 21081(a)(2)(A). HAVA requires this auditable record to be a "permanent paper record" but does not require it to be produced before vote casting so that voters can verify its contents. § 21081(a)(2)(B)(i); s*ee also infra* Section V.A.

180. 52 U.S.C. § 21081(a)(3)(A). HAVA led to important efforts to improve the accessibility of voting, but much progress remains to be made. Moreover, "[t]here will never be a single perfect voting machine that meets everyone's accessible-voting needs." RUNYAN, *supra* note 99, at 3; *see also infra* Section VI.A.

181. 52 U.S.C. § 21081(a)(5).

182. 52 U.S.C. § 21082.

183. 52 U.S.C. § 21083.

casting and counting votes."[184] HAVA's initial allocation was $650 million, with a provision for additional subsequent appropriations.[185]

Finally, Title II of HAVA sets up the EAC, a new agency charged with overseeing HAVA's implementation. Notably, the EAC is tasked with "provid[ing] for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories," in conjunction with the National Institute of Standards and Technology.[186] States may opt to, but are not required to, use this accredited certification.[187] Additionally, Title II has multiple provisions aiming to improve future election administration and technology: Subtitle C provides that the EAC "shall conduct and make . . . public studies regarding . . . the election administration issues . . . with the goal of promoting . . . convenien[ce], accessib[ility], and eas[e of] use . . . [as well as] the most accurate, secure, and expeditious system for voting and tabulating election results."[188] Subtitle D provides for "grants to assist entities in carrying out research and development to improve the quality, reliability, accuracy, accessibility, affordability, and security of voting equipment, election systems, and voting technology,"[189] and "pilot programs under which new technologies in voting systems and equipment are tested and implemented on a trial basis so that the results of such tests and trials are reported to Congress."[190]

An important feature of HAVA regarding voting machines is its requirement that all punch card and lever voting machines were to be replaced by the next federal election (then, 2004), although exceptions were permitted for good cause. While it was beneficial to phase out the problematic punch card and lever machines, this initiative unexpectedly backfired in terms of security as the replacement machines were often DRE machines[191] that are now disfavored due to security and auditability concerns.[192] DRE machines were explicitly

184. 52 U.S.C. §§ 20901(b)(1)(F), 20903.
185. 52 U.S.C. §§ 20904(a), 20930.
186. 52 U.S.C. § 20971(a)(1).
187. 52 U.S.C. § 20971(a)(2).
188. 52 U.S.C. § 20981(a).
189. 52 U.S.C. § 21041(a).
190. 52 U.S.C. § 21051(a).
191. NAS REPORT, *supra* note 2, at 77.
192. *See* Tokaji, *supra* note 140, at 1739; NAS REPORT, *supra* note 2, at 77–79, 88, 109–10; JONES & SIMONS, *supra* note 3, at 108–11; Lawrence Norden & Andrea

recommended, and also favored for their accessibility features, in HAVA itself.[193] Subsection IV.B.3 provides further discussion of the evolution of understanding of the security risks of DRE machines over time.

State statutory requirements. State election codes generally specify requirements for voter qualifications, voter registration, nominating candidates, early voting, absentee voting, military voting, appointment and removal of election personnel, districting, what kinds of questions may appear on the ballot, and election-related crimes.[194] State election codes also impose some constraints on ballot design, voting equipment, and polling place setup and management.[195] Within the constraints of state (and federal) law, local officials have broad discretion to make administrative decisions.[196]

Regarding election security, state election codes often specify rules—or specify the body, such as a board of elections, that is authorized to make rules—about ballot secrecy at polling places; adoption, testing, and other technical requirements on voting technology; security of voter registration systems; procedures to identify voters and verify their registration; public observation of election processes; procedures to challenge alleged irregularities in election administration; and any post-election audit requirements.[197] While all state election codes include some such provisions, some states' codes are less detailed than others and may lack provisions regarding many of the above aspects. Notably, many states require new voting equipment to conform to federal guidelines (which are only advisory unless states choose to adopt some or all of them as mandatory).[198]

Córdova McCadney, *Voting Machines at Risk: Where We Stand Today*, BRENNAN CTR. FOR JUST. (Mar. 5, 2019), https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-where-we-stand-today [https://perma.cc/4JMA-KDUY].

193. 52 U.S.C. § 21081.

194. *See generally* N.Y. ELEC. LAW §§ 1-100 to 17-222 (McKinney 2021).

195. *See generally id.*

196. *See* HANNAH FURSTENBERG-BECKMAN ET AL., ASH CTR. FOR DEMOCRATIC GOVERNANCE AND INNOVATION, UNDERSTANDING THE ROLE OF LOCAL ELECTION OFFICIALS: HOW LOCAL AUTONOMY SHAPES U.S. ELECTION ADMINISTRATION 8–16 (2021), https://ash.harvard.edu/files/ash/files/role_of_local_election_officials.pdf [https://perma.cc/NS4J-Z7WD].

197. *See, e.g.*, N.Y. ELEC. LAW §§ 8-300, 7-200, 7-201, 7-202, 7-206, 3-103, 5-206, 6-208, 17, 9-211 (McKinney 2021).

198. *See Voting System Standards, Testing and Certification*, NAT'L CONF. OF STATE LEGISLATURES (Nov. 5, 2021),

IV. A CONSTITUTIONAL RIGHT TO VOTE SECURELY

We often conceptualize the act of voting as the act of placing a ballot in a box, but this conception is deceptively simplistic when considering the right to vote. The Supreme Court has "repeatedly recognized"[199] that the Constitution protects not just "the right to put a ballot in a box"[200] but rather the right to cast an "effective[]" vote[201] "for the candidate of one's choice"[202] that "must be correctly counted and reported."[203] In the words of leading election law scholars, "Exercising the right to vote effectively requires that voters' intentions be recorded and counted accurately."[204] What happens after the ballot goes in the box is just as important as access to the ballot box and the placing of the ballot in the box—in other words, casting a ballot is meaningless if the ballot box is a dumpster on fire.

Most U.S. voting rights litigation to date has focused on practices that disenfranchise voters by preventing them from even casting a ballot. This is unsurprising given a long history of outright "deny[ing] or restrict[ing] the right of suffrage"[205] for particular groups of people, and given that, for centuries, the system of placing a paper ballot in a physical ballot box meant that methods for tampering with ballots after casting were relatively limited and not very scalable.[206] Still, the Supreme Court's earliest voting rights cases[207]—as well as common sense and common usage of the term "vote"—recognize that casting, counting, and reporting are all essential components of the right to vote.

---

https://web.archive.org/web/20221031215426/https://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx [https://perma.cc/3HLV-3TH2].

199. Reynold*s* v. Sims, 377 U.S. 533, 554 (1964) ("It has been repeatedly recognized that all qualified voters have a constitutionally protected right to vote, and to have their votes counted.") (citations omitted); *see also, e.g.*, 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 . . . .").

200. Gray v. Sanders, 372 U.S. 368, 380 (1963) (quoting United States v. Mosley, 238 U.S. 383, 386 (1915)); *see also Reynolds*, 377 U.S. at 555 n.29 (quoting South v. Peters, 339 U.S. 276, 279 (1950) (Douglas, J., dissenting)).

201. Williams v. Rhodes, 393 U.S. 23, 30 (1968).

202. *Reynolds*, 377 U.S. at 555; Burdick v. Takushi, 504 U.S. 428, 441 (1992).

203. *Gray*, 372 U.S. at 380.

204. LOWENSTEIN ET AL., *supra* note 73, at 398.

205. *Reynolds*, 377 U.S. at 554.

206. *See also infra* note 302.

207. *See* cases cited *supra* notes 199–202.

Today, the relevance of disenfranchisement at the counting and reporting stages—after the ballot goes in the box—has grown dramatically with the introduction of complex technologies for ballot casting, tallying, and reporting. Such technologies introduce the potential for mishaps and misconduct in the tallying process that are much more complex, scalable, and difficult to detect. Disenfranchisement after casting—that is, not counting a ballot towards the eventual election outcome after allowing a voter to cast it—devalues a person's vote just as much as if they had never cast it and indeed can be more insidious and harder to litigate than denying access to the ballot, as it can be done without the disenfranchised person ever finding out. In light of this, constitutional voting rights jurisprudence needs to develop a more detailed approach to voting rights violations *after* ballot casting. This Part aims to develop such an approach in the specific context of election system security.

As noted earlier, there are at least three federal constitutional voting rights doctrines under which a constitutional right to vote *securely* might naturally arise: (1) the *Anderson-Burdick* balancing test for burdens on the right to vote, (2) *Bush v. Gore*'s prohibition of arbitrary and disparate treatment of voters, and (3) vote dilution.

A. Insecure Technology As a Burden on Voting Rights Under Anderson-Burdick

Recall that in the *Anderson-Burdick* balancing test, the level of scrutiny applicable to a challenge to an election regulation depends on the magnitude of the burden it places on voting rights.[208] In practice, essentially any election regulation is treated as a burden on voting rights that triggers the balancing test.[209] The facts of the seminal cases that apply the test make clear that burdens under *Anderson-Burdick* need not directly encumber the act of casting a vote. Rather, burdens under *Anderson-Burdick* have been construed broadly to mean any impediment upon the free and effective exercise of the franchise.

208. Anderson v. Celebrezze, 460 U.S. 780 (1983); Burdick v. Takushi, 504 U.S. 428 (1992).

209. *Burdick*, 504 U.S. at 434 (quoting Norman v. Reed, 502 U.S. 279, 288–89 (1992)).

Thus, all of the real doctrinal work is done in the balancing—each burden must be justified by relevant and legitimate state interests "sufficiently weighty to justify the limitation."[210] Whether such burdens are constitutional depends on whether the state adequately justifies them based on legitimate state interests.[211]

1. The Sliding Scale

In more detail, the *Anderson-Burdick* balancing test requires courts to weigh (1) the burden imposed against (2) the State interests offered as justification and (3) how necessary or narrowly tailored the election regulation is to serve the stated interests.[212]

While "severe" burdens are subject to strict scrutiny—that is, a severely burdensome regulation must be "narrowly drawn to advance a state interest of compelling importance"[213]—the proper treatment of lesser burdens have been less precisely articulated by the Supreme Court. *Burdick* stated simply that "the State's important regulatory interests are generally sufficient to justify [reasonable, nondiscriminatory] restrictions."[214] *Burdick*'s phrasing appears to establish an intermediate scrutiny requiring "important" state interests. *Burdick* emphasizes that the state interests asserted were "legitimate" and "sufficient to outweigh the limited burden" imposed by the challenged ban on write-in voting, and that the ban was "a reasonable way of accomplishing [the State's] goal[s]."[215]

On the other end of the sliding scale, the Sixth Circuit has applied rational-basis review[216] to "minimally burdensome and

210. Crawford v. Marion Cnty. Election Bd., 553 U.S. 181, 191 (quoting *Norman*, 502 U.S. at 288–89).

211. *Anderson*, 460 U.S. at 796; *Burdick*, 504 U.S. at 440.

212. *Burdick*, 504 U.S. at 428 ("A court considering a state election law challenge must weigh the character and magnitude of the asserted injury to the First and Fourteenth Amendment rights . . . against the precise interests put forward by the State as justification for the burden imposed . . . taking into consideration the extent to which those interests make it necessary to burden the plaintiff's rights.").

213. *Id.*

214. *Id.* at 434 (quoting *Anderson*, 460 U.S. at 788).

215. *Id.* at 440.

216. Or alternatively, sometimes, "a less-searching examination closer to rational basis." Ohio Council 8 Am. Fed'n of State v. Husted (*Husted III*), 814 F.3d 329, 335 (6th Cir. 2016).

nondiscriminatory" election regulations,[217] contrasting them with "regulations that impose a more-than-minimal but less-than-severe burden," which are subject to *Burdick* and *Crawford*'s intermediate scrutiny.[218] This Sixth Circuit approach is consistent with *Crawford*'s lead opinion but diverges from a concurrence that argues that *Anderson-Burdick* establishes just two scrutiny levels.[219]

2. Insecure Election Technology Is a Burden on the Right to Vote

Mandating the use of insecure election technology qualifies as a burden under *Burdick*'s "however slight" threshold test.[220] A voter whose vote is deleted, miscounted, or ignored due to a security failure has been completely deprived of their vote, so an insecure election system creates the burden that *a voter's vote is at heightened risk of not being properly counted*.

As discussed earlier, the Supreme Court has consistently held that the right to vote encompasses both the right to cast a vote and the right to have it "correctly counted and reported."[221] However, fact patterns of *Anderson-Burdick* cases to date have centered on burdens at earlier stages of the voting process: burdens on vote-casting or, earlier yet, burdens on ballot access by minor candidates or parties.[222] This focus is unsurprising. First, the bulk of U.S. voting rights litigation has for decades focused on who can cast a vote at all, and how to ensure equal vote-casting opportunities for all—rightly so, against a backdrop of widespread discrimination denying many even these initial steps. Secondly, for much of U.S. history, vote counting has been done by manual inspection of paper ballots (with accompanying security and transparency measures). This is an uncontroversial procedure that provides a credible and easily understood

217. Green Party of Tenn. V. Hargett (*Hargett I*), 767 F.3d 533, 546 (6th Cir. 2014); *see also Husted III*, 814 F.3d at 335; Husted II, 834 F.3d 620, 627 (6th Cir. 2016).

218. *Husted II*, 834 F.3d at 627 (quoting *Hargett I*, 767 F.3d at 546).

219. Crawford v. Marion Cnty. Election Bd., 553 U.S. 181, 204–05 (2006) (Scalia, J., concurring in the judgment).

220. *Id.* at 191.

221. Gray v. Sanders, 372 U.S. 368, 380 (1963).

222. The concededly indirect burden on the right to vote from limiting candidate access to the ballot is well established to be within the *Anderson-Burdick* doctrine's scope, starting from *Anderson* itself.

guarantee that, once cast, ballots will be counted and reported in the final tally.

The increasing use of modern technology has gradually brought into issue whether our election systems provide adequate assurance that ballots are correctly counted and reported *after* casting.[223] "The nature of threats to election systems is changing as state and non-state actors attempt to undermine election systems through cyber and information warfare."[224]

Happily, the analytical approach of past *Anderson-Burdick* cases in assessing burden severity focuses broadly on the right to vote, and thus applies just as well to burdens at later stages of the election process. A unified analytical approach to burdens at all stages of the voting process seems only natural, considering that the casting, counting, and reporting of votes are each necessary steps toward realizing the fundamental right to vote that *Anderson-Burdick* is designed to protect.

It may seem unusual to treat as redressable the fact of a heightened risk. The more familiar approach common in many legal domains is to redress realized risks, rather than potential risks not yet realized. Yet *Anderson-Burdick*'s deliberately broad and conceptual formulation of burdens on voting rights not only permits but seems to require the treatment of insecure election infrastructure as a burden—even though its immediate impact is a potential harm whose precise likelihood may not admit quantification and even though the specific harm of miscounting votes might not be realized at all. Anderson's own burden—an early filing deadline for independent candidates—can be viewed similarly. It gave rise to the heightened risk of Anderson's campaign being less successful if he was not listed on the ballot (so his supporters had to write in his name). The precise likelihood of lesser success could not be quantified, and the potential harm might not have been realized at all had Anderson's supporters all written in his name come Election Day. Indeed, Anderson's supporters' likelihood of getting their preferred candidate elected was arguably *entirely unchanged* by the restriction, given that he was an independent candidate for president.

Anderson-Burdick's broad formulation is no accident. Rather, it responds to the specific and heightened demands that

223. *See supra* Sections II.C, II.D.

224. NAS REPORT, *supra* note 2, at 119.

we make of election systems, as the vehicles that realize the constitutional right to vote. It is only natural for the doctrine to err on the side of inclusivity, opening the door to burdens "however slight," given: (1) the risk of grave, irreparable, and perhaps undetectable and unprovable damage in case of underinclusivity and (2) that what counts as a burden does not determine constitutionality, but simply induces further analysis in the form of the balancing test that constitutes the bulk of *Anderson-Burdick* analyses in practice. The risks of grave, irreparable, undetectable, and unprovable damage are a common feature of other areas of law that recognize heightened risk as a redressable injury in itself, as discussed in Section IV.D, as well as in computer security research in general, as discussed in Section II.F.

3. Sufficiently Insecure Election Infrastructure Fails the *Anderson-Burdick* Test

Having determined that insecure voting technology burdens the right to vote, the next steps under *Anderson-Burdick* are to determine the severity of the burden, then determine whether state interests justify the burden at the corresponding level of scrutiny. This Subsection argues that insecure election technology can, in some cases, so burden voting rights as to warrant strict scrutiny and that sufficiently insecure election technology would fail strict scrutiny.

The burden imposed by any given technology is fact-specific. The purpose of this Subsection is not to assess a specific technology's constitutionality in specific circumstances but rather to demonstrate that uses of election technology may realistically be so insecure as to be unconstitutional under *Anderson-Burdick*. I therefore consider a generalized hypothetical where an election authority deploys technology that is well established to have serious security flaws. The analysis assumes that this insecure technology is the primary voting method, it does not produce a paper audit trail, and alternative methods of voting are either unavailable or significantly more inconvenient.

a. Type of Burden

Anderson-Burdick cases have consistently treated burdens tantamount to disenfranchisement as "severe" burdens subject

to strict scrutiny and have classified as "limited" burdens those that are reasonably described as inconveniences, easily avoidable, or "not a significant increase over the usual" burdens of voting.[225]

Insecure election technology facilitates omission and miscounting of ballots during the tallying process, potentially surreptitiously and at large scale. Its use imposes two distinct kinds of burden on voting rights, which I categorize under *realized risk* and *potential risk*. I assume below that the use of the technology at issue is not also discriminatory (that would be a separate ground for strict scrutiny).[226]

Realized-risk burdens. First, any voters whose ballots were dropped or miscounted have suffered a burden on the right to have their vote counted and reported in the election outcome—a burden that literally disenfranchises and is thus "severe." Such voters are burdened by the *realized risk* of their vote not being counted. It may be difficult for such voters to find out or prove that they specifically were disenfranchised—an issue with concerning evidentiary and standing implications. But the burden on these particular voters is severe and thus would merit strict scrutiny.

To give a simple example that avoids most of the evidentiary issues, suppose that after a busy day at the polls, poll workers checked the information stored in their electronic voting machine: "–1 vote cast."[227] Then, all voters who used the

225. *Crawford*, 553 U.S. at 184.

226. Under *Anderson-Burdick*, discriminatory election practices merit strict scrutiny regardless of the severity of the burden. The Court has not precisely defined the meaning of "discriminatory" in this context. In general, mandating the use of insecure election technology facially impacts all voters and does not facilitate tampering with the votes of certain classes of voters more than others. However, insecure election technology could conceivably be designed to discriminate. A more likely scenario is that insecure election technologies, even if not consciously designed to be discriminatory, will nonetheless disproportionately disadvantage the poor and technologically less literate. While this is a deeply concerning consideration that should factor into policy decisions, today's courts seem unlikely to treat disadvantaging the poor as cause for heightened scrutiny under *Anderson-Burdick*. *But see id.* at 236 (Souter, J., dissenting) ("If more were needed to condemn this law, our own precedent would provide it, for . . . the Indiana statute crosses a line when it targets the poor and the weak.").

227. Similar situations have been documented in practice. For example, in the 2004 presidential election, a "machine malfunction wiped out some 4,500 votes in local races in Carteret County, N.C." John Schwartz, *Mostly Good Reviews for Electronic Voting*, N.Y. TIMES (Nov. 12, 2004), https://www.nytimes.com/2004/11/12/pageoneplus/mostly-good-reviews-for-electronic-voting.html [https://perma.cc/MPK4-PSK9]. Fortunately, in these particular cases, the errors were detected and thus able to be corrected.

machine would have been disenfranchised as their votes were not recorded or tallied—a severe burden.

Potential-risk burdens. Secondly, all eligible voters have suffered the serious harm of having to be part of an electoral process that is not "necessarily structured to maintain the integrity of the democratic system,"[228] in which voters lack meaningful assurance (1) that cast ballots are correctly counted and reported generally and (2) that their own ballots specifically are correctly tallied. Even if it is unclear—or perhaps impossible to know—whether a particular voter's ballot has been dropped or miscounted, that voter has nonetheless suffered the serious harm of being subjected to potential risk—that is, subjected to significant objective uncertainty[229] over whether their vote (or anyone else's) will be correctly counted and reported, and consequently whether their democratic system will function correctly.[230]

b. Severity of Burden

As discussed in Subsection IV.A.2, past cases have focused on burdens on vote *casting* or earlier stages of the electoral process. Such cases tend to give rise to *realized-risk* burdens. Realized-risk burdens from insecure election infrastructure can be severe, as already noted above.

The case law lacks fact-specific examples of assessing the severity of *potential-risk* burdens. As noted above, *Anderson* itself is the primary example of an *Anderson-Burdick* analysis of a potential-risk harm.

The familiar paradigm of realized-risk burdens may tempt one to assess the severity of potential-risk burdens indirectly by considering the severity of the realized-risk harm that it might lead to (e.g., by assessing the likelihood of risk realization and the severity of harm in case it does realize). But on the contrary, *Anderson* tells us that the severity of potential-risk burdens should be assessed directly, treating the *imposition of potential risk* as a burden in itself, not indirectly by assessing the likelihood and severity of the corresponding realized risk. Tellingly, the *Anderson* court did not concern itself with

228. Burdick v. Takushi, 504 U.S. 428, 441 (1991).

229. Throughout this Section, the term "uncertainty" refers to objective uncertainty arising from the factual circumstances of unreliability in an election system, rather than subjective uncertainty perceived by individuals.

230. *See also infra* Subsection IV.A.2.d.

probabilities of specific realized harm. Instead, it analyzed burden severity by assessing the challenged restriction's direct impact—that is, the severity of the very imposition of potential risk.[231]

To illustrate the same principle in a more concrete, if less realistic, example, imagine a polling place where, in order to enter, voters must walk through a metal detector that is known to be defective. It causes mild but painful burns in roughly one in a million people. The burden on voting rights of such a system is not adequately characterized by considering just the severity of the burns and the likelihood that a voter is actually hurt. Rather, it is embodied in the direct burden on every voter who is obliged to walk through the detector at risk of harm simply in order to exercise their voting rights—a burden on even those who go through unscathed.

Can the potential risk inherent in insecure election infrastructure, then, be so severe as to be tantamount to disenfranchisement? I argue that in egregious cases, yes, as the hypotheticals that follow aim to illustrate. Specifically, (1) an unreliable tallying process can, in severe cases, be tantamount to disenfranchisement, and (2) an election system that creates a substantial chance that many cast ballots will not be correctly counted and reflected in the election outcome can devalue the correct counting and reporting of ballots as much as one that outright omits or miscounts ballots. The following hypotheticals are deliberately simplistic; they are designed to be as simple as possible while capturing the essential concepts of uncertainty in tallying to support the preceding two conclusions.

Consider an election where voters are choosing between two candidates and that has the following tallying process: For each ballot cast, a coin is flipped. If the coin comes up heads, a vote is recorded for the candidate indicated on the ballot, but if it comes up tails, a vote is recorded for the *other* candidate. Such a tallying system would severely burden voting rights—and this would be so even if the earlier parts of the election system perfectly allowed every eligible voter to easily cast a ballot. The burden is tantamount to disenfranchisement because subjecting the counting of ballots to such uncertainty as embodied in a coin flip devalues correct counting just as much as outright omitting

231. *E.g.*, Anderson v. Celebrezze, 460 U.S. 780, 790 (1992) (noting that an "early filing deadline may have a substantial impact on independent-minded voters").

or miscounting them. From another perspective, the burden is also tantamount to disenfranchisement for another reason: the ballots cast have no impact on the election outcome (in a strict mathematical sense, as well as intuitively speaking).[232]

Realistic election systems are very unlikely to have perfectly known amounts of uncertainty, and usually the uncertainty in a system also depends on unknown human behavior. To give an alternate hypothetical better illustrating the unknown nature of uncertainty in real systems, consider a system where, for each box of cast ballots, an election worker asks for a volunteer in the street to seal up the box and transport it to a counting location across town. Again, the burden is tantamount to disenfranchisement because subjecting the ballots to such uncertainty as entailed by entrusting them to unknown volunteers devalues the correct counting of the ballots comparably to outright omitting or miscounting them. This is so even though no meaningful analysis of the probability that ballots will be correctly counted is possible; an election system that creates great objective uncertainty as to the accuracy of counting devalues the integrity of the election process as much as does an election system that makes it clear that votes are likely to be miscounted. The foregoing analysis remains unchanged even if in practice most volunteers promptly deliver their boxes intact, and so actually, nearly all the ballots are correctly counted. The last observation underscores that the core of the burden is in the imposition of potential risk, so the proper focus should be at least as much on the systemic harm to voters who are left with substantial uncertainty as to whether they were disenfranchised as on one who was *actually* disenfranchised.

For systems where the chance of miscounting is so substantial that one might describe the tallying process as largely up to chance, or up to human caprice, such as in the two hypotheticals above, the burden imposed seems tantamount to disenfranchisement, and strict scrutiny appears appropriate. More limited unreliability in the tallying process could perhaps—if significantly less harmful than disenfranchisement and reasonably described as merely inconvenient or easily

232. The coin flip scheme means one's vote does not make one's preferred candidate any more likely to be elected since *exactly the same procedure would have been followed* had one voted for the other candidate. Ultimately, no matter how many people vote and who they vote for, there is a random one-half chance of each candidate's election.

avoidable by voters—be a limited burden that merits *Burdick*-style intermediate scrutiny.

c. Strict Scrutiny Analysis

To be upheld, election regulations that are subject to strict scrutiny must be "narrowly tailored to advance a compelling state interest."[233] "[I]f there are other, reasonable ways to achieve [the state's] goals with a lesser burden on constitutionally protected activity, a state may not choose the way of greater interference."[234]

The state interests that have been asserted in the few challenges to insecure election technology so far are: (1) administrative convenience (including cost efficiency) of continuing to use existing equipment[235] and (2) accessibility for voters with disabilities.[236] Another conceivable interest would be convenience or ease of use (arguably promoting turnout)—though, to my knowledge, this interest has not been asserted so far.

In some cases, including the recent Georgia litigation, administrative convenience was the *only* interest asserted by the state.[237] Courts have consistently treated administrative convenience as an insufficiently compelling state interest to pass even intermediate scrutiny, both in the context of insecure election technology[238] and in many other areas of constitutional law.[239] In certain cases, courts have even pronounced the continued use of election technology that is well-established to have serious vulnerabilities to be "unreasonable" and have "no rational basis."[240] The state interest in administrative convenience is thus inadequate to justify the use of insecure election technology under strict or intermediate scrutiny.

233. *Burdick*, 504 U.S. at 433.

234. Dunn v. Blumstein, 405 U.S. 330, 343 (1972).

235. *E.g.*, Stewart v. Blackwell, 444 F.3d 843, 869 (6th Cir. 2006).

236. *E.g.*, Wexler v. Anderson, 452 F.3d 1226, 1233 (11th Cir. 2006).

237. *See Stewart*, 444 F.3d at 869; Curling v. Kemp, 334 F. Supp. 3d 1303, 1324 (N.D. Ga. 2018).

238. *See Stewart*, 444 F.3d at 869; *Kemp*, 334 F. Supp. 3d at 1324.

239. *E.g.*, Reed v. Reed, 404 U.S. 71 (1971).

240. Sw. Voter Registration Educ. Project v. Shelley, 344 F.3d 882, 900 (9th Cir. 2003); Common Cause S. Christian Leadership v. Jones, 213 F. Supp. 2d 1106, 1109 (C.D. Cal. 2001). In these cases, the insecure technologies were used in the presence of other more secure alternative technologies.

The second proposed interest, accessibility for disabled voters, is an important one. But in the case of very serious vulnerabilities, the stated regard for disabled voters' interests backfires. It cannot be described as a compelling state interest—arguably, it cannot even be described as having a rational basis—to provide voters with disabilities with equipment so flawed as to cause severe uncertainty about whether their votes, though perhaps easily cast, will be counted at all.[241]

When an election technology has severe vulnerabilities casting serious doubt on the accurate tallying of ballots, attempting to justify its use by its accessibility for voters with disabilities is fallacious in a similar way to arguing for the use of the paper airplane voting system with the added feature that voters with disabilities will have accessibility devices that will help them fill out, fold, and toss their paper airplane ballots out of the window, all from the convenience of their homes. It is true that such a system could make casting a ballot easier for many voters with disabilities. But it is also true that such a system would harm, not improve, their chances of casting an *effective* vote that is reflected in the election outcome—the purpose of casting a vote in the first place.

In many contexts, a fine-grained balancing between accessibility benefits for voters with disabilities and the security risks of the technology that provides enhanced accessibility could be appropriate under an *Anderson-Burdick* analysis. However, if a particular proposal for an accessible system is very insecure, its adoption may come at the cost of a meaningful assurance that votes will be counted, defeating the purpose of providing the accessible system to begin with[242]—that is, to facilitate participation by voters with disabilities in the electoral process. Similar reasoning applies to the state interests in promoting accessibility or turnout for the electorate at large, regardless of disability.

In sum, the accessibility of casting an *effective* vote—where casting is accompanied by a meaningful assurance that cast votes will be counted—is a compelling state interest that could pass strict scrutiny depending on the context, whether for voters with disabilities or voters in general. But an accessible but

241. *See infra* note 309.

242. Attempts to provide accessibility at the cost of fundamentally altering or undermining the basic purpose of a facility do not meaningfully achieve accessibility. This concept also relates to the fundamental alteration doctrine in disability law. *See* PGA Tour, Inc. v. Martin, 532 U.S. 661, 682 (2001).

severely insecure system may undermine the chance of cast votes being counted, and thus be far from tailored to further the compelling state interest of making the casting of effective votes accessible.

B. Insecure Technology as Arbitrary and Disparate Treatment Under Bush v. Gore

In *Bush v. Gore*, the Supreme Court held that the Equal Protection Clause prohibits a state from running an election system that, "by . . . arbitrary and disparate treatment, value[s] one person's vote over that of another" or imposes election procedures that cause an "unequal evaluation of ballots" cast by different voters.[243] Much *Bush v. Gore* litigation to date has focused on differential treatment of voters in different *geographic* locations (usually, county-level variations). But *Bush v. Gore* itself did not depend on the fact that different counties took different approaches; it was the disparate treatment of voters' ballots that created a Fourteenth Amendment issue. Indeed, *Bush v. Gore* mentioned the possibility of disparate treatment of different ballots within the same county based on nongeographic factors.[244]

Cases challenging election technology for arbitrary and disparate treatment, to date, have argued that different voters using different equipment are treated arbitrarily and disparately as a result of differences in the equipment used. Subsection IV.B.1 discusses this theory in more detail. Subsection IV.B.2 expounds a new theory that different voters using the *same* insecure election technology can suffer arbitrary and disparate treatment under the meaning of *Bush v. Gore*.

1. Arbitrary and Disparate Treatment of Different Voters Using Different Technologies

Bush v. Gore precedents indicate that a state's use of an insecure election technology for some votes alongside a more secure alternative for others could amount to unconstitutional

243. Bush v. Gore, 531 U.S. 98, 104–06 (2000).

244. *Id.* at 106 ("[T]he standards for accepting or rejecting contested ballots might vary not only from county to county but indeed within a single county from one recount team to another . . . and . . . at least one county changed its evaluative standards during the counting process.").

arbitrary and disparate treatment,[245] and subsequent academic commentary lends further support to this conclusion.[246] Election-technology precedents suggest that, at least where the insecure equipment is well-known to have serious vulnerabilities, its continued use alongside better alternatives is likely unconstitutional. The arbitrary and disparate treatment in such cases (like in *Stewart*)[247] would be between those voters provided with more secure voting technology and those provided with less secure technology, who are arbitrarily subjected to significantly different probabilities of their votes being accurately counted and reported in the election outcome.

Such cases would fit especially neatly into the framework of *Bush v. Gore* and *Gray* if the different technologies were in different geographic areas. But modern cases have shifted the analytical focus from geographic disparity to disparate treatment more broadly—including specifically in the context of challenges to unreliable election technology—so that disparate treatment between voters using different technologies in the same location seems quite likely to be treated as a *Bush v. Gore*-style constitutional harm as well. That said, realistically, wherever multiple election technologies are deployed, geographic disparities are likely. County-level election officials tend to have discretion in managing election equipment, and studies indicate that county-level variation in election technology is widespread.[248]

The above reasoning does not imply that the Constitution mandates the use of the same election technology statewide[249]—no more than *Bush v. Gore* mandates that the same human being inspect all the ballots in Florida for the sake of uniformity. Rather, the above reasoning comports with the idea that "local

245. *See* Stewart v. Blackwell, 444 F.3d 843 (6th Cir. 2006); *Jones*, 213 F. Supp. 2d 1106; Black v. McGuffage, 209 F. Supp. 2d 889 (N.D. Ill. 2002).

246. *See* Schwartz, *supra* note 105; Richard B. Saphire & Paul Moke, *Litigating* Bush v. Gore *in the States: Dual Voting Systems and the Fourteenth Amendment*, 51 VILLANOVA L. REV. 229 (2006); Richard L. Hasen, Bush v. Gore *and the Future of Equal Protection Law in Elections*, 29 FLA. ST. U. L. REV. 377 (2002).

247. *See supra* Section III.A.

248. David Card & Enrico Moretti, *Does Voting Technology Affect Election Outcomes? Touch-Screen Voting and the 2004 Presidential Election*, 89 REV. ECON. & STAT. 660, 669 (2006).

249. In this respect, the reasoning in this Section is more conservative than some more expansive proposed interpretations of *Bush v. Gore*. *See* Hasen, *supra* note 246, at 395 ("In sum, if *Bush v. Gore* indeed has precedential value, it clearly should apply to prevent the use of . . . different voting systems [with different error rates] in the same election.").

entities, in the exercise of their expertise, may develop different systems for implementing elections."[250] *Bush v. Gore* and subsequent cases make clear that the election practices proscribed by *Bush v. Gore* are not just any differences in treatment of different voters, but treatment that is both *disparate* in such a manner and to such an extent as to implicate nontrivial curtailment of the fundamental right to vote, and *arbitrary* meaning that it is not the product of a reasoned policy, as would be a local entity's reasonable decision "in the exercise of their expertise." As long as multiple election technologies deployed by a state are comparable in security, or as long as any discrepancies are explained by reasoned policy decisions, they would be permitted under *Bush v. Gore*. However, statewide policies or standards for testing and auditing election equipment could help local authorities exercise their expertise and discretion in choosing election technology while also ensuring equitable treatment of voters across the state, within *Bush v. Gore*'s constitutional bounds.

2. Arbitrary and Disparate Treatment of Different Voters Using the Same Technology

Past cases and scholarship provide less guidance on whether the reasoning of *Bush v. Gore* could extend to the treatment of different voters using the *same* insecure election technology to vote. This is perhaps unsurprising; where, as often, insecure election technology is deployed alongside a preferable, more secure technology, the argument that voters using *different* technology are arbitrarily and disparately treated may seem the easier one to make. However, the uniform use of a single insecure election technology could give rise to an arbitrary and disparate treatment claim *closer to* the original reasoning of *Bush v. Gore* than a different-technology claim.

In *Bush v. Gore*, the Florida Supreme Court had prescribed a standard for manually evaluating voter intent based on ballot markings: to consider "the intent of the voter." This standard was simple and facially uniform. According to the U.S. Supreme Court, the Florida Supreme Court's standard *facially* failed to

250. Bush v. Gore, 531 U.S. 98, 109 (2000); *see also id.* at 134 (Souter, J., dissenting) ("It is true that the Equal Protection Clause does not forbid the use of a variety of voting mechanisms within a jurisdiction, even though different mechanisms will have different levels of effectiveness in recording voters' intentions . . . .").

guarantee sufficiently consistent evaluation of ballots as to ensure equal protection for all Florida voters.

Bush v. Gore has not been extended to as-applied challenges. Instead, the doctrine has so far recognized facial challenges to election practices of two types: (1) those that facially call for differential treatment of different voters, resulting in arbitrary and disparate treatment, and (2) those that facially fail to provide sufficient guarantees of nonarbitrary or disparate treatment of voters in such a way that arbitrary and disparate treatment is a natural and inevitable consequence in practice—for example, by being overly vague or subjective.

The second type, while more indirect, is the subject of *Bush v. Gore* itself. As described above, the procedure prescribed by the Florida Supreme Court was a simple, facially uniform standard.[251] The U.S. Supreme Court considered this "unobjectionable as an abstract proposition and a starting principle. The problem inheres in the absence of specific standards to ensure its equal application. The formulation of uniform rules to determine intent based on [ballot markings] is practicable and . . . necessary."[252] Equal protection, the Court explained, requires states to employ election practices with "minimal . . . safeguards" to provide "at least some assurance that the rudimentary requirements of equal treatment and fundamental fairness are satisfied."[253] Based on this and similar reasoning, the Court held Florida's ballot evaluation procedure to be "[in]consistent with [the state's] obligation to avoid arbitrary and disparate treatment of [voters]," a "minimum requirement . . . necessary to secure the fundamental right" to vote.[254]

To exemplify the sort of arbitrary and disparate treatment that resulted from Florida's "standardless" rule, the Court noted that "each of the counties used varying standards to determine what was a legal vote," and "at least one county changed its evaluative standards during the counting process."[255] Notwithstanding such references to as-applied effects, however, the Court's reasoning focused squarely on the inadequate guidance and inadequate protection against arbitrary treatment

251. *Id.* at 105 (internal quotation marks omitted).
252. *Id.* at 105–06.
253. *Id.* at 109.
254. *Id.* at 105.
255. *Id.* at 106–07.

inherent in Florida's rule, and ultimately reached a facial determination of unconstitutionality.

Just like the "intent of the voter" ballot evaluation procedure in *Bush v. Gore*, deploying a single insecure election technology statewide would be a simple, facially uniform practice: every voter would use the same technology to vote. But, just as in *Bush v. Gore*, this facially uniform practice would fail to "satisfy the minimum [constitutional] requirement for nonarbitrary treatment of voters" because the election procedure that it prescribes is inherently of such a nature—that is, so insecure—as to cause arbitrary and disparate treatment of voters as an all but necessary consequence in practice.

The paper airplane voting system illustrates this reasoning. Facially, it treats all voters uniformly: each voter casts their vote using the same procedure of casting a paper airplane into the street, and the high-tech ballot material and instructions are provided equally to all voters. However, the design of the system for casting votes is so insecure that arbitrary and disparate treatment of ballots once cast is a practically inevitable consequence.

It is also true, both in *Bush v. Gore* and in the paper airplane system, that the state-imposed rules are facially *compatible* with nondisparate treatment of voters—for example, if all poll workers happened to employ the same method of determining voter intent or if each legitimately cast paper airplane ballot happened to be collected and counted intact. But notwithstanding any such bare compatibility, the Court in *Bush v. Gore* determined that when an election practice almost certainly causes arbitrary and disparate treatment in practice, it does not meet the "minimum [constitutional] requirement for nonarbitrary treatment" and is facially invalid. Accordingly, the paper airplane voting system should be held unconstitutional for arbitrary and disparate treatment of voters by the same logic employed in *Bush v. Gore* itself.

The idea that the use of a single election technology can lead to "inevitable . . . errors" due to the technology's inherent unreliability was also mentioned by the Sixth Circuit in *Stewart*, while discussing punch card technology where "running . . . ballots repeated[ly] through the counting machinery will result in different results."[256] *Stewart* involved the use of this

256. Stewart v. Blackwell, 444 F.3d 843, 855 (6th Cir. 2006) (internal quotation marks omitted) (discussing standing).

unreliable technology alongside other more reliable technology and ultimately took the analytically simpler path of invalidating the election regulations at issue for arbitrary and disparate treatment of different voters using *different* technologies to vote. However, had the unreliable punch card technology been deployed uniformly statewide, it could still have been held unconstitutional under *Bush v. Gore*'s theory of near-inevitable arbitrary and disparate treatment caused by a facially uniform election practice that provides inadequate "safeguards . . . to assure the rudimentary requirements of equal treatment."

3. Advances in Our Understanding of Insecure Voting Technology Since *Stewart*

Security experts' understanding of the strengths and weaknesses of technologies evolves over time. The evolution in understanding is generally a one-way street; technologies once believed to be reliable may be shown to be insecure, and may become outdated and superseded by newer technologies, but there is no way to redeem a technology once it is demonstrated to be vulnerable. The best we can hope for is to create new technologies that leverage our understanding of past vulnerabilities to achieve better security.

Such shifts in understanding can be dramatic. For example, the type of voting machine—DRE—that was upheld in *Stewart* as the preferable, more reliable technology is the very same technology that the Secretary of the Department of Homeland Security declared in 2018 to be a "national security concern."[257] By 2018, that technology was only in use in five states[258] and was under legal challenge for causing a "serious risk" that votes "may be altered, diluted, or effectively not counted" in Georgia.[259]

This state of affairs may seem frustrating and unpredictable. But every legal dispute can only, at best, be decided based on the best scientific (and lay) knowledge available at the time of adjudication. Given the rapid pace of technological advancement, this means that election equipment upheld in one case may be invalidated in a subsequent case. Ultimately, this is a desirable outcome, in that the law

257. *See* Curling v. Kemp, 334 F. Supp. 3d 1303, 1311 (N.D. Ga. 2018).
258. *See id.* at 1324.
259. *See id.* at 1325.

incorporates sufficient flexibility to respond to changing scientific knowledge on a question that inherently depends on the context and state of the art—that is, how to adequately secure election systems and realize the constitutional right to vote.[260]

That said, it is beneficial for courts to explicitly take into account the likelihood of change to the extent possible, especially for new and untested technologies which may not yet be ripe for deployment even given positive preliminary assessments. In the computer security community, a new technology's security properties are not considered credible until it has demonstrated resilience over an extended period of testing and real-world deployment. At least with respect to security-critical infrastructure like election technology, courts might improve the consistency and reliability of their decisions by adopting an analogous presumption that new and relatively untested technologies be treated as insecure until a substantial base of evidence, including independent research over an extended period, creates a broad and high-confidence consensus on its security within the expert community.[261]

C. Insecure Technology as Vote Dilution

Vote dilution refers to diminishing the relative weight of certain voters' votes compared to others without preventing voters from casting ballots.[262] Historically, districting has been the main mechanism by which the relative weights of votes are changed, in which context a number of election practices that cause vote dilution have been held unconstitutional.[263]

The use of insecure election technology can also be described in the language of vote dilution. For example, "[o]verweighing and overvaluation of the votes of those living in a county with

260. Other contexts in which changing scientific knowledge bears upon legal questions have also taken an adaptive approach. *See* MICHAEL LYNCH ET AL., TRUTH MACHINE: THE CONTENTIOUS HISTORY OF DNA FINGERPRINTING (2008); KENNETH R. FOSTER & PETER W. HUBER, JUDGING SCIENCE: SCIENTIFIC KNOWLEDGE AND THE FEDERAL COURTS (1997).

261. While it is generally not possible to irrefutably prove technologies secure, it is possible to build a solid foundation of evidence of an acceptable level of security that would yield high confidence among security experts.

262. *See, e.g.*, LOWENSTEIN ET AL., *supra* note 73, at 216.

263. *See* Reynolds v. Sims, 377 U.S. 533 (1964); White v. Regester, 412 U.S. 755 (1973); Davis v. Bandemer, 478 U.S. 109 (1986); Nicholas O. Stephanopoulos, *The New Vote Dilution*, 96 N.Y.U. L. REV. 1179 (2021).

adequate technology has the certain effect of dilution and undervaluation of the voters of those living in a county with deficient technology,"[264] and "when [plaintiffs] vote [using insecure equipment], their vote is in jeopardy of being counted less accurately and thus given less weight than a paper ballot."[265]

Challenges to insecure election technology do not fit into the districting-based conceptions of vote dilution that have for decades been recognized by the Supreme Court, but they fit remarkably well into an emerging new category of vote dilution claims—"vote dilution through fraud facilitation"[266]—that have arguably begun to see recognition in lower courts[267] and may gain broader recognition over time.

In a recent article observing that "[w]e may currently be witnessing the emergence of a [new] category of vote dilution claims" and expounding how vote dilution through fraud facilitation has appeared in cases to date, as well as arguing how it ought to work, Nicholas Stephanopoulos distilled the analysis of vote dilution by fraud facilitation into two steps.[268] "First, an overly lax voting rule induces electoral fraud. Second, the resulting fraud cancels out votes that are lawfully cast. Therefore, the overly lax policy is unconstitutional—dilutive of honest citizens' valid votes."[269]

This analytical framework would apply admirably to some important objections to the use of insecure election technology, supposing courts recognize this type of claim. First, insecure election technology induces heightened risk of inaccurate tallying. Second, the resulting inaccuracies cancel out votes that are lawfully cast. Therefore, the use of insecure election technology is unconstitutionally dilutive of legitimate votes.

Is there a compelling reason for this theory of vote dilution to cover deliberate fraud but exclude unreliability due to non-fraudulent errors? The similarity in dilutive *effect* of fraud and non-fraudulent errors in the context of insecure election technology raises a compelling argument to recognize the effect of non-fraudulent errors as vote dilution too. In both cases, the result is that some ballots are accurately counted and others are

264. Stewart v. Blackwell, 444 F.3d 843, 870 (6th Cir. 2006).
265. Curling v. Kemp, 334 F. Supp. 3d 1303, 1325 (N.D. Ga. 2018).
266. Stephanopoulos, *supra* note 263, at 1181.
267. *See id.*
268. *Id.* at 1180.
269. *Id.*

not, and the influence of the inaccurately tallied ballots is unjustly diluted relative to the influence of the accurately tallied ones. The unconstitutional state conduct is that of *facilitating* such dilution of votes by providing an election system that makes such dilution likely.

D. Insecure Election Systems Give Rise to a Directly Redressable Harm

Some may argue that demonstrating the mere existence of vulnerabilities is speculative and thus insufficient to present a problem amenable to legal redress, absent solid evidence about the likelihood of the vulnerabilities being exploited in a given election. But, as discussed above in the context of *Anderson-Burdick*, the direct harm of operating insecure election equipment is in the potential risk it represents—risk that exists at the time of operation, independently of whether vulnerabilities are subsequently exploited (i.e., whether the potential risk is realized). Recognizing the harm of imposing this potential risk *before the risk realizes* is essential to ensure the secure conduct of elections—and far more effective than recognizing the harm of miscounting after the fact—since (1) misconduct can be hard to detect or prove, by the very reason of insecurity, leaving voters without recourse, and (2) the procedural harms can be challenged and stopped long before the election, with enough time to fix problems without undue election disruption, and in a "less provocative [manner] since it doesn't occur in the heat of an election, when the consequences for different candidates are clear to everyone."[270]

There are plenty of legal contexts in which undertaking an unreasonable risk is in itself proscribed—where the reasonableness of risk is quantified not by the (perhaps unquantifiable) likelihood of its realization, but rather by the nature of the risk and the cost of mitigation. In the election context, *Bush v. Gore* found an equal protection violation based on flawed election procedures even "in the absence of any evidence that a definable class of voters had been treated unfairly."[271] But examples abound in other areas of law too. In

270. *Id.* at 1196.

271. Tokaji, *supra* note 140, at 1749, 1752 ("*Bush* identifies the procedures and mechanisms used to conduct elections—and more specifically the vote-counting process—as the proper subject of an equal protection challenge."); *see also* discussion *supra* Subsection IV.B.2 (discussing *Bush v. Gore* in more detail).

national security, financial regulation, data protection, and food and drug safety—to name just a few—the failure to take adequate precautions to reduce risk is often actionable regardless of whether the risk has been realized. In many such contexts, the likelihood of realization of the risk is not meaningfully quantifiable, just as for insecure election equipment—for example, the likelihood that classified information will actually be misused if widely disclosed, the precise amount of financial loss that would result from bank transactions being unsecured, the likelihood that poorly protected personal data will actually be used for identity fraud, or the likelihood that products that do not follow FDA safety procedures will in fact harm consumers. Instead, what determines the level of precaution we require in these contexts is how easy it would be to misuse the classified information or personal data if it were released or poorly protected, how easy it would be to steal money if bank transactions were poorly secured, and how easy it would be to sell harmful products for consumption if FDA safety procedures were not in place. These, unlike the probability of actual abuse, are quantifiable. Such an approach also mirrors the common technical approach—discussed in Section II.F—of assessing the severity of vulnerabilities based on technically quantifiable factors that determine how easy they would be to exploit, rather than based on the more uncertain *likelihood* of exploitation. The analogous measure in the context of election system security is the severity of the vulnerabilities, that is, *how easy it would be* to corrupt the election if one so desired.

The idea that insecurity alone is too speculative to be redressable may come from several sources. First, the familiar paradigm of tort law makes actionable only risky conduct that actually results in concrete harm to an individual (except in certain special cases). This is a policy choice in the specific context of torts, not borne out in many other areas of law. Tort cases are "backward-looking" in that they seek to compensate the injured for realized risk. Even among tort cases, there are certain contexts where a risk is considered itself to be a serious injury and proof of the usual tort elements is unusually difficult due to the nature of the harm, such that courts grant relief based on unrealized risk, for example, toxic torts.[272]

272. *See* Jamie A. Grodsky, *Genomics and Toxic Torts: Dismantling the Risk-Injury Divide*, 59 STAN. L. REV. 1671, 1678–79 (2007); Ayers v. Township of

Second, another source of concern about the speculative nature of litigation based on election infrastructure insecurity may be the classic worry about opening the floodgates to frivolous cases based on unfounded speculation. In Section VI.B, I explain why I believe such frivolous litigation will in fact be easily distinguished and discarded. Furthermore, even if frivolous cases are a valid reason for caution in the *litigation* context, this should not impede the passage of *legislation* imposing specific requirements on election equipment. Indeed, legislating clear election-security rules should reduce litigation by giving election officials greater clarity about their duties.

Finally, the direct harm associated with insecure election equipment may be less intuitive than the other kinds of risks that are established to be directly redressable due to the complex technology involved—perhaps creating the impression to the public of a more speculative or ill-defined harm than in other comparable contexts. The ease of exploitation of widely distributed classified information or personal data, the financial risk of unsecured bank transactions, and the ease of selling harmful food and drugs in an unregulated market are more intuitive to a broader audience than the ease of exploitation of complex election infrastructure—especially for equipment that appears superficially to function adequately, but which experts opaquely evaluate to have serious vulnerabilities. Of course, not all examples of insecure election infrastructure involve complex technology,[273] but most realistic ones do.

In summary, operation of election infrastructure with known serious vulnerabilities should be a redressable harm on its own, quantifiable based on the severity of the *vulnerabilities*, independent of whether those vulnerabilities are in fact exploited on a given occasion. The former is a potential-risk harm, the latter is a realized-risk harm, and each should be redressed in its own right with appropriate forms of remedies.

E. Discussion

In sum, challenges to insecure election infrastructure fit the existing analytical frameworks of *Anderson-Burdick* or *Bush v.*

Jackson, 106 N.J. 557, 592 (1987) ("[A]n enhanced risk of disease caused by significant exposure to toxic chemicals is clearly an 'injury' . . . .").

273. For example, consider storing ballots in a windy unfenced parking lot overnight before tallying.

Gore, and courts could hold certain insecure technologies unconstitutional under these doctrines, especially in egregious cases. But courts are unlikely to treat insecure election infrastructure as causing unconstitutional vote dilution unless the new category of vote dilution by fraud facilitation is recognized.

Past election-technology challenges have more often invoked *Bush v. Gore*. However, *Anderson-Burdick* is a far longer-standing voting-rights doctrine that covers a far broader range of case law with more established precedential value in the Supreme Court,[274] and its focus on *burdens* rather than *disparate treatment* is closer to the core problem with insecure election technology and the manner in which its use infringes upon the right to vote. *Anderson-Burdick* is the most versatile doctrine of the three, likely applicable to the widest range of challenges to insecure election technology.

* * *

Many significant details remain to be worked out regarding how the theories would apply to insecure election practices, including standing, evidentiary requirements, and remedies—full details of which are beyond this Article's scope. These issues will be complicated where poor security makes it difficult to determine whether and how problems occurred during an election.

Fortunately, the limited case law already exhibits some promising trends. First, courts have consistently recognized the standing of plaintiff voters in past challenges to election technology with serious vulnerabilities (under *Bush v. Gore* or *Anderson-Burdick*) without proof that those particular plaintiffs' votes were miscounted or unusually impacted[275]—a seemingly necessary approach to standing in the context of insecure election infrastructure, as obtaining such evidence might be impossible for the very reason of the election infrastructure's

274. *See supra* note 158.

275. *See* Stewart v. Blackwell, 444 F.3d 843, 854 (6th Cir. 2006) ("[C]ourts have [long] recognize[d] that the increased risk of harm constitutes an injury sufficient to support standing."); Wexler v. Anderson, 452 F.3d 1226 (11th Cir. 2006); Curling v. Kemp, 334 F. Supp. 3d 1303 (N.D. Ga. 2018). *But see* Donald J. Trump for President, Inc. v. Boockvar, 493 F. Supp. 3d 331 (W.D. Pa. 2020); Donald J. Trump for President, Inc. v. Cegavske, 488 F. Supp. 3d 993 (D. Nev. 2020); Wood v. Raffensperger, 501 F. Supp. 3d 1310 (N.D. Ga. 2020).

insecurity. Secondly, courts have treated as plausible both remedies related to specific past elections to redress realized-risk burdens or harms (e.g., recounting mishandled ballots before certification of results) and preemptive remedies related to future election procedures for potential-risk burdens or harms (e.g., requiring improved security measures in future), but they have rejected plaintiffs' attempts to obtain election-specific remedies for alleged potential-risk harms (e.g., preventing or reversing certification of results, or postponing elections, based on alleged uncertainty about fraud or tallying).[276] Thirdly, courts are mindful that election litigation must not become a political tool for last-minute disruption of elections, and consistently protect ongoing and imminent elections from disruption, both during litigation and when granting relief that may impact future election administration.[277]

* * *

Constitutional litigation is an important backstop that could provide protection from egregiously insecure election systems in the absence of any additional legislation. But it is an inefficient vehicle for realizing secure elections in practice. First, the baseline level of security that is required by the Constitution is not enough to bring election systems up to date with modern security best practices. Secondly, enforcement by constitutional litigation is contingent on aptly positioned plaintiffs choosing to sue and can create cross-jurisdictional variations and uncertainty that may persist over years absent appellate review. Litigation may inefficiently tie up judicial resources and draw out public uncertainty about election security over the pendency of a case. Thirdly, the conduct of federal elections was explicitly assigned to Congress's discretion—and elections and election security can be politically fraught—so the legislative branch has much broader authority to issue detailed guidelines for the conduct of elections than the judicial branch. Fourthly, court opinions are a poor vehicle for issuing comprehensive

276. *Compare Stewart*, 444 F.3d 843, *with* Donald J. Trump for President, Inc. v. Boockvar, 502 F. Supp. 3d 899 (M.D. Pa. 2020), *and* Bowyer v. Ducey, 506 F. Supp. 3d 699, 706–07 (D. Ariz. 2020), *and* Sw. Voter Registration Educ. Project v. Shelley, 344 F.3d 882, at 900, 919–20 (9th Cir. 2003).

277. *See* Purcell v. Gonzalez, 549 U.S. 1, 4–5 (2006); RNC v. DNC, 140 S. Ct. 1205 (2020); *Kemp*, 334 F. Supp. 3d 1303; Curling v. Raffensperger, 493 F. Supp. 3d 1264 (N.D. Ga. 2020).

requirements on election system security, both because of their inherently limited binding scope and because the relevant technical expertise is the domain of legislators and agencies more than judges. Lastly, there is a limit to how much under-resourced election offices can improve their systems simply because a court decision mandated it; substantial improvements need funding and oversight from legislation.

New election security legislation may also have the indirect benefit of systematizing the security practices that legislators and experts today can agree that modern election systems should meet, thus providing a reference for courts in assessing the security of challenged systems in any constitutional challenges that do still arise.

The next Part turns to legislative approaches.

V. THE ROLE OF THE LAW IN ELECTION SECURITY

To date, federal law has played a limited role in securing elections. The influence of state law on election infrastructure security, though greater than that of federal law, has also been secondary to the discretionary decisions of state and local election bodies.[278]

As election systems face ever-more-sophisticated threats from an ever-growing range of actors, the law will need to play a greater role in securing our elections in casting, counting, and checking. The right to vote has always been "a fundamental political right, [] preservative of all rights"[279]—that has not changed. But threats to voting rights have evolved and grown in complexity over time, and legal mechanisms to protect voting rights should evolve to meet them.

Historically, in the United States, the greatest threats to the right to vote have related to disenfranchisement of specific subpopulations such as women and racial minorities—for example, denial of voting rights or candidature;[280] targeted voter intimidation;[281] devices designed to prevent voting by

278. *See generally* KATHLEEN HALE ET AL., ADMINISTERING ELECTIONS: HOW AMERICAN ELECTIONS WORK 27–51 (2015).

279. Yick Wo v. Hopkins, 118 U.S. 356, 370 (1886).

280. *E.g.*, Nixon v. Herndon, 273 U.S. 536 (1927).

281. *E.g.*, Giles v. Harris, 189 U.S. 475 (1903).

specific groups, such as literacy tests;[282] and gerrymandering.[283] Such threats, and measures to counteract them, have largely been driven domestically. Today, the introduction of modern technology into our election infrastructure has created a much larger attack surface for more sophisticated, remotely controlled, and harder-to-detect attacks, including attacks from abroad, limited instances of which have been documented in practice.[284]

Concerns about election integrity spiked in the wake of doubts about the way the election was conducted in recent controversial elections—notably 2000, 2016, and 2020.[285] Reliability and public confidence in the system is more important than ever in controversial elections, and in recent years we have seen the system struggle to provide the kind of assurance the public seeks.[286] This state of affairs seems unlikely to change meaningfully without legal or regulatory intervention given that: the entrenched election equipment ecosystem has allowed technology long shown to be insecure to remain in use with vulnerabilities unaddressed; the market is dominated by just a handful of powerful vendors;[287] and under-resourced local election offices too often lack the funding,

282. *See* Lassiter v. Northampton Bd. of Elections, 360 U.S. 45 (1959); Harper v. Va. Bd. of Elections, 383 U.S. 663 (1966); Kramer v. Union Free Sch. Dist., 395 U.S. 621 (1969).

283. *See* Baker v. Carr, 369 U.S. 186 (1962); Davis v. Bandemer, 478 U.S. 109 (1986); Vieth v. Jubelirer, 541 U.S. 267 (2004).

284. MUELLER REPORT, *supra* note 42. Other countries are experiencing similar issues. *See* Melissa Eddy, *Germany Investigates Russia over Pre-Election Hacking*, N.Y. TIMES (Sept. 20, 2021), https://www.nytimes.com/2021/09/10/world/europe/germany-russia-hacking-investigation.html [https://perma.cc/X7WW-HJ36]; Laurens Cerulus, *Europe's Most Hackable Election*, POLITICO.EU (Jan. 16, 2019), https://www.politico.eu/article/europe-most-hackable-election-voter-security-catalonia-european-parliament-disinformation [https://perma.cc/WAH2-C6AX].

285. *See* Leslie Wayne, *The 2000 Election: The Voting System*, N.Y. TIMES (Nov. 10, 2000), https://www.nytimes.com/2000/11/10/us/the-2000-election-the-voting-system-close-vote-illuminates-hodgepodge-of-ballots.html [https://perma.cc/WKF8-NH97]; MUELLER REPORT, *supra* note 42; NAS REPORT, *supra* note 2, at xi–xii; Eric Geller, *Forget the Conspiracy Theories—Here Are the Real Election Security Lessons of 2020*, POLITICO (Dec. 27, 2020), https://www.politico.com/news/2020/12/27/election-security-lessons-2020-450356 [https://perma.cc/6QBH-HXEM].

286. *See generally supra* note 285; NAS REPORT, *supra* note 2, at 122 ("If the challenges currently facing our election systems are ignored, we risk an erosion of confidence in our elections system and in the integrity of our election processes.").

287. CAULFIELD ET AL., *supra* note 34, at 6; NAS REPORT, *supra* note 2, at 45–46, 110–15.

administrative freedom, and/or technical expertise to conduct meaningful security evaluations even for the equipment available in this suboptimal market.[288]

It may be illuminating to consider the evolution of the legal system's role in cases of racial discrimination. Early protection of voting rights against racial discrimination was established through constitutional litigation.[289] Then in the VRA, Congress recognized the ongoing threat to voting rights and responded by requiring and proscribing specific conduct to better protect the right to vote against racial discrimination and created an individual right of action to challenge discriminatory denial or abridgment of voting rights.[290] Much subsequent litigation relied on the VRA, gradually resulting in a body of case law that led to meaningful change and improvement.[291]

The threat posed by insecure election infrastructure is still in relatively early stages of recognition and incorporation into legal protections. Litigation and public concern about insecure election equipment has been noticeable, and occasionally prominent, since 2000. Though HAVA was intended to address some election security concerns, it "provides only limited guidance on what type of voting equipment should be implemented, with few binding mandates."[292] HAVA did not introduce robust and enforceable protections comparable to those of the VRA.

Today, twenty years after HAVA, we have learned important lessons about federal election legislation. "[I]t is

288. *See* NAS REPORT, *supra* note 2, at xii, 38, 108; CHARLES STEWART III, NAT'L INST. FOR CIV. DISCOURSE, THE COST OF CONDUCTING ELECTIONS (2022), https://electionlab.mit.edu/sites/default/files/2022-05/TheCostofConductingElections-2022.pdf [https://perma.cc/LSH9-WQ4T].

289. *E.g.*, Nixon v. Herndon, 273 U.S. 536 (1927).

290. *See generally* CONG. RES. SERV., THE VOTING RIGHTS ACT OF 1965: BACKGROUND AND OVERVIEW (2015), https://crsreports.congress.gov/product/pdf/R/R43626/15 [https://perma.cc/LC8T-ZGYQ].

291. *See, e.g.*, *Impacts of the Voting Rights Act and the Supreme Court's Shelby Ruling*, HARV. KENNEDY SCH. (Oct. 26, 2018), https://www.hks.harvard.edu/faculty-research/policy-topics/politics/impacts-voting-rights-act-and-supreme-courts-shelby-ruling [https://perma.cc/2WAQ-VBG9]. *But see* Michael Li & Sonali Seth, *The Coming SCOTUS Fight over the Voting Rights Act*, BRENNAN CTR. FOR JUST. (Sept. 21, 2022), https://www.brennancenter.org/our-work/analysis-opinion/coming-scotus-fight-over-voting-rights-act [https://perma.cc/DM3S-UYBD] (discussing how an upcoming U.S. Supreme Court decision may render previously impactful VRA provisions much less effective).

292. Tokaji, *supra* note 140, at 1734.

imperative that election reform no longer be thought of as a once-in-a-generation occurrence."[293] We have weathered new kinds of controversies over election outcomes, some arising from the use of newer voting technologies than those at issue in *Bush v. Gore*. And there is "growing concern about the aging of voting systems purchased after HAVA, which are now over a decade old."[294]

The time seems right for legislation that will strengthen election integrity, provide recourse against the continuing use of outdated and vulnerable election equipment, and provide resources to local election authorities to maintain equipment that meets security best practices into the future. Indeed, multiple legislative proposals have been made in the last several years, though none have yet passed.[295] Lawmakers on both sides of the aisle have expressed serious concerns about election security,[296] though they have framed those concerns differently based on partisan considerations.

The remainder of this Part describes key elements related to election-system security that would be beneficial for new legislation to mandate:[297] (1) accessible, secrecy-preserving voting methods that produce reliable *voter-verifiable evidence* of each voter's cast vote, in a format that is not susceptible to alteration or destruction in an undetectable fashion or at large scale; (2) *detailed public information* about all technology and processes essential to the correct functioning of an election; (3) public *audits* of all such technology, and post-election audits to confirm reported outcomes; (4) security best practices for other election system components beyond casting and tallying, such as voter registration and election-night reporting; and (5) enhanced feedback mechanisms between election security experts,

293. *Id.* at 1716.

294. LOWENSTEIN ET AL., *supra* note 73, at 401; *see also* NAS REPORT, *supra* note 2, at 92; Matthew M. Damschroder, *Of Money, Machines, and Management: Election Administration from an Administrator's Perspective*, 12 ELECTION L.J. 195 (2013).

295. *See* For the People Act of 2021, H.R. 1, 117th Cong. (2021); Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019); Election Security Assistance Act, H.R. 3412, 116th Cong. (2019).

296. Evidenced by proposed legislation from both sides of the aisle. *See supra* note 295.

297. Congress's constitutional authority for such mandates would arise from the Spending Clause (under which states may decline the money and ignore the mandate) and Congress's power to determine the manner of conduct of federal elections. *See* Jennifer Nou, supra note 11, at 781–82; Franita Tolson, *The Spectrum of Congressional Authority over Elections*, 99 B.U. L. REV. 317, 378 (2019).

accessibility and usability experts, and election officials, including reporting and investigation of security incidents. The later sections of this Part discuss measures necessary to facilitate the implementation of the above mandates including (1) voter information and education and (2) funding and designation of agencies responsible for implementing the legislation. For ease of reference, in the discussion below, I call the hypothetical new legislation "the Act."

A. Durable Voter-Verifiable Evidence of Cast Votes

The Act should require all election systems to produce durable voter-verifiable evidence of cast votes. Voters must be able to personally verify the *authoritative record* of their vote that will be used for counting and auditing, and that record must be in a *durable* format that is likely to persist unchanged throughout the election (and as long as needed afterwards), is difficult to tamper with at scale, and is likely to show signs of modification if modified.

Voter-marked paper ballots straightforwardly satisfy the verifiability requirement; voters mark their ballots themselves, and those same ballots serve as the authoritative record of their votes. But if voters use a device or intermediary to mark their ballots, the verifiability requirement becomes more subtle. Machine-marked ballots where the authoritative record (e.g., on paper) is subsequently verified and cast directly by the voter satisfy the requirement. However, machine-marked ballots where the authoritative record is not verifiable by the voter do *not* satisfy the requirement—for example, a touchscreen voting machine where votes are recorded electronically. In systems that do not produce voter-verifiable evidence of cast votes—much as if someone else filled out the voter's ballot, allegedly according to the voter's instructions,[298] and cast it without letting the voter see or handle the ballot—voters cannot be sure whether the authoritative record that they have never observed matches their intentions.[299]

298. Putting aside ballot secrecy for a moment.

299. Additional verification procedures cannot cure this defect *unless they allow the voter to directly verify their authoritative vote record*. For example, if a touchscreen machine offered an on-screen review of the voter's choices before vote casting or if the person who filled out the ballot claimed to read back the voter's choices, the resulting systems would still not satisfy voter verifiability since the review is detached from the authoritative record.

This concept is often called "voter-verified paper audit trail" (abbreviated as VVPT or VVPAT) or "contemporaneous paper record." These terms all feature the word "paper," reflecting the current state of the art in security. Despite decades of research and development effort, paper remains the only[300] currently known way to implement durable voter-verifiable evidence of votes, and appears quite likely to remain so for years to come.[301] Paper's key properties are human-readability, durability, tamper-evidence, and difficulty of manipulation at scale.[302] Of course, paper is far from foolproof, and fraudsters have devised many creative ways to tamper with paper ballots over the centuries;[303] however, paper provides stronger durability and tamper-evidence properties than other known data storage media, especially with respect to *large-scale* errors or tampering.

That said, the Act should frame its mandates in terms of the technical security requirements that must be achieved by voting technologies, rather than naming specific voting methods. Such framing will facilitate flexible adaptation to future technological developments.[304] The requirement of voter-verifiable evidence of cast votes is supported by recent legislative proposals,[305] academic commentary in law and computer science,[306] and multiple organizations that study election security and policy.[307]

The Act should also strengthen HAVA's accessibility requirements. While HAVA originally included DRE machines

300. Similar alternatives such as cardstock would do as well. *See infra* note 301.

301. *See* NAS REPORT, *supra* note 2, at 95; Park et al., *supra* note 72, at 3; Appel & Stark, *supra* note 11, at 525. The use of paper records alone is not enough; the paper records must be *voter verifiable* before casting and they must be the *authoritative record*. Thus, it is not enough to print out paper ballots after electronic casting or to keep paper backups of an electronic record where the latter is treated as authoritative.

302. Paper is not the only medium satisfying these properties, but it is one of the most practical for use. Ballots made of cloth, card, or plastic could also satisfy these properties. However, purely electronic storage media do not. *See* NAS REPORT, *supra* note 2, at 94–95.

303. *See, e.g.*, JONES & SIMONS, *supra* note 3, at 39–41.

304. *See* Tokaji, *supra* note 140, at 1716 (arguing against "legislative bodies . . . mandating any particular technological fix").

305. *See* Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019); For the People Act of 2021, H.R. 1, 117th Cong. (2021).

306. *See* Rivest, *supra* note 76; Appel & Stark, *supra* note 11; Simons, *supra* note 38; Park et al., *supra* note 72; Richard L. Hasen, *Identifying and Minimizing the Risk of Election Subversion and Stolen Elections in the Contemporary United States*, 135 HARV. L. REV. FORUM (2022).

307. *See* NAS REPORT, *supra* note 2, at 6–7; *Brennan Ctr. Recommendations*, *supra* note 61.

as an example of an acceptable accessible voting technology, DREs (especially paperless DREs) have since been established to have serious security vulnerabilities and thus are now disfavored.[308] It could be seen as an unintended loophole of HAVA that it allowed the provision of "accessible" voting technologies that are easier for at least some to use,[309] but are also so insecure as to create a seriously elevated risk that the votes of those using the provided technologies will not be properly counted.[310] But of course, the idea of accessibility and the stated intention of HAVA is to provide an accessible technology that performs the *same or comparable* functionality as the non-accessible counterpart—not an inferior functionality that puts those using the accessible technology at risk.[311]

The Act should therefore (1) explicitly exclude accessible technologies that risk devaluing the votes cast using them, instead requiring that voters who use accessible technologies, too, enjoy *commensurate secrecy, independence, verifiability, and integrity guarantees to a hand-marked paper ballot*, and (2) make sure that accessible technologies do not compromise the secret ballot by ensuring that accessible technologies are widely used across the electorate. These strengthened requirements would mean that paperless DREs (and other insecure DREs) would no longer meet statutory requirements. A likely and beneficial side effect would be that the accessible technologies developed to meet these requirements[312] will streamline voting even for those who could use a traditional hand-marked paper ballot.[313]

---

308. *See* sources cited *supra* note 192.

309. *See* RUNYAN, *supra* note 99, at 8.

310. *Hearing on S.B. 1723 Before the Sen. Elections & Reapportionment Comm.*, 2003–2004 Leg. Sess. (Cal. 2004) (statement of Natalie Wormeli) ("Not having the ability to vote without another human being's assistance is the reality that I deal with . . . . [Some] disability rights advocates claim that decertification [of DREs] would be a step back, treating people with disabilities as second class citizens. I argue that requiring California voters to use dangerously flawed DREs will be forcing second rate technology on us all.").

311. This idea is arguably also implicit in the "fundamental alteration" doctrine of disability law. PGA Tour v. Martin, 532 U.S. 661 (2001).

312. At the time of writing, the existing technology most suitable to meet these requirements is ballot-marking devices. *See* sources cited *supra* note 103.

313. *See* Emens, *supra* note 104.

B. Open Election Technology

Today, election technology is highly secretive.[314] This is counterproductive in several ways: (1) it is bad for security, as elaborated below; (2) it frustrates the important goal of providing *credible public assurance* that the system functions as intended and any errors will be caught (i.e., the checking guarantee); and (3) it appears to harm interoperability and innovation, as evidenced by the slow-changing equipment in the current oligopoly market of players established for more than a century.[315]

Of these, the first point is perhaps least intuitive—how can hiding system designs harm security? Open access to system designs promotes "independent technical evaluation of voting systems that, in turn, facilitates oversight and accountability."[316] Conversely, preventing scrutiny of and "hiding . . . vulnerabilities in [systems] decreases the likelihood [that they] will be repaired and increases the likelihood that they . . . will be exploited by evil-doers."[317] Some modern security experts opine that "public scrutiny is the only reliable way to improve security" as it enables wider scrutiny, particularly by those who are the most incentivized to check a system and be assured of its correct functioning—typically, not the vendors.[318]

---

314. *See* NAS REPORT, *supra* note 2, at 46.

315. *See* JONES & SIMONS, *supra* note 3, at 37; Brenda Reddix-Smalls, *Individual Liberties and Intellectual Property Protection—Proprietary Software in Digital Electronic Voting Machines: The Clash Between a Private Right and a Public Good in an Oligopolistic Market*, 19 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 689 (2009); NAS REPORT, *supra* note 2, at 45, 110–15; Tokaji, *supra* note 139, at 1806; Nou, *supra* note 11, at 757, 760, 779.

316. Joseph Lorenzo Hall, *Transparency and Access to Source Code in Electronic Voting*, USENIX/ACCURATE ELEC. VOTING TECH. WORKSHOP 3 (2006).

317. Steven M. Bellovin & Randy Bush, *Security Through Obscurity Considered Dangerous*, THE INTERNET SOCIETY (2002) (manuscript), https://www.cs.columbia.edu/~smb/papers/draft-ymbk-obscurity-00.txt [https://perma.cc/WP8Z-A8GN]; *see also* Auguste Kerckhoffs, *La Cryptographie Militaire*, 4 J. DES SCIS. MILITAIRES 5 (1883); Saltzer & Shroeder, *supra* note 69, at 1282; Anna Shipman, *Don't Be Afraid to Code in the Open: Here's How to Do It Securely*, GOV.UK (Sept. 27, 2019), https://technology.blog.gov.uk/2017/09/27/dont-be-afraid-to-code-in-the-open-heres-how-to-do-it-securely [https://perma.cc/R7SC-C8E9]; Rebecca T. Mercuri & Peter G. Neumann, *Security by Obscurity*, 46 COMMC'NS OF THE ACM 160 (2003).

318. *See* Bruce Schneier, *The Non-Security of Secrecy*, 47 COMMC'NS OF THE ACM 120 (2004); Whitfield Diffie, *Risky Business: Keeping Security a Secret*, ZDNET (Jan. 16, 2003), https://www.zdnet.com/article/risky-business-keeping-security-a-secret-5000127072 [https://perma.cc/BSJ8-Q3TC]. Others opine that "[w]hile not publishing details of security mechanisms is perfectly acceptable as one security

"Flaws cannot be fixed if they are not properly understood, and the modern history of technology repeatedly reminds us that we rely on the presumed ignorance of attackers only at great peril."[319] In other words, to be secure against sophisticated adversaries, a system should be secure even when how it works (but not the sensitive data it handles) is transparent to the attacker—a tried and tested security principle that dates back as far as the nineteenth century and is still widely referenced today.[320]

The Act should require full public disclosure of the design and manufacture (including supply chains) of any technology that is to play an essential role in the correct functioning of an election, including source code. Recent, relatively small-scale pilots have demonstrated the preliminary viability of open-source voting systems, though they have not yet gained substantial market traction.[321] Furthermore, the Act should require full public disclosure of any chain of custody records, audit logs, and other internal state, inputs, or outputs that are reasonably necessary to verify the correct functioning of such technology. The Act should mandate such transparency as a condition of government contracts for election technology,[322] thus barring any intellectual property claims that vendors might otherwise make against transparency. Enhancing election technology transparency has also been advocated by academics in law and computer science,[323] organizations that study

mechanism, it is perhaps the one most easily breached, especially in this age of widespread information dissemination"—and thus, that security must not *depend* on secrecy. Matt Bishop, U.C. Davis, *Overview of Red Team Reports*, *in* CAL. SEC'Y OF STATE TOP-TO-BOTTOM REVIEW, *supra* note 3.

319. David Wagner, U.C. Berkeley, *Principal Investigator's Statement on Protection of Security-Sensitive Information*, *in* CAL. SEC'Y OF STATE TOP-TO-BOTTOM REVIEW, *supra* note 3.

320. *See* sources cited *supra* note 317.

321. *See* Lucas Laursen, *What Open Source Technology Can and Can't Do to Fix Elections*, IEEE SPECTRUM (Apr. 27, 2020), https://spectrum.ieee.org/what-open-source-technology-can-cant-do-fix-elections [https://perma.cc/2U3P-3MVD]; VOTINGWORKS, https://www.voting.works [https://perma.cc/PSF2-UB5E].

322. California has required disclosure of designs and documentation to the Secretary of State as a condition of voting machine certification. *See* JONES & SIMONS, *supra* note 3, at 199.

323. *See* Reddix-Smalls, *supra* note 315; Hall, *supra* note 316; Tokaji, *supra* note 140, at 1794.

election security and policy,[324] and coalitions of election officials.[325]

A transition period may be necessary before full public disclosure mandates take effect. If so, then during the transition period, full disclosure of all the above information should still be required at least to election officials, the EAC, CISA, and to any independent third-party auditors commissioned by any of the preceding parties.[326]

Election technology vendors may express concern that such measures would disrupt their business models or security, but (1) as observed above, the current business models appear inadequate to meet modern election security requirements if left alone, and (2) the consensus of security experts is that disclosing such logs and internal information is necessary for security,[327] and that truly secure systems need not rely on the secrecy of their designs.[328] Concerns about disruption to business models are often followed by innovative adaptations. But if it is really the case that the election technology market would be undermined by the proposed measures, then one explanation is that the current market relies on under-resourced election offices overpaying for insecure technology that could be outcompeted by more secure and affordable products but for the

---

324. *E.g.*, SALTMAN, *supra* note 16; ELECTION VERIFICATION NETWORK, TEN THINGS ELECTION OFFICIALS CAN DO TO HELP SECURE AND INSPIRE CONFIDENCE IN THIS FALL'S ELECTIONS 1 (2016), https://electionverification.org/wp-content/uploads/2014/11/EVN-Top-Ten-List.pdf [https://perma.cc/6TNT-4D97]; *Principles for New Voting Systems*, VERIFIED VOTING (Feb. 1, 2015), https://verifiedvoting.org/publication/principles-for-new-voting-systems [https://perma.cc/W64G-HMPP]; Peter Wolf, *Election Technology: Precondition for Transparent Elections or Pretext for Questioning Electoral Integrity?*, INT'L INST. FOR DEMOCRACY & ELECTORAL ASSISTANCE (Sept. 27, 2017), https://www.idea.int/news-media/news/election-technology-precondition-transparent-elections-or-pretext-questioning [https://perma.cc/8E9G-4Z6C]; Kim Zetter, *DARPA Is Building a $10 Million, Open Source, Secure Voting System*, VICE (Mar. 14, 2019), https://www.vice.com/en/article/yw84q7/darpa-is-building-a-dollar10-million-open-source-secure-voting-system [https://perma.cc/GP3N-QE29]; *see also* Shipman, *supra* note 317.

325. *See* NAS REPORT, *supra* note 2, at 111.

326. *See* Hall, *supra* note 316, at 14 (also suggesting disclosure to selected independent experts).

327. *See, e.g.*, Ams. for Safe Access v. Cnty. of Alameda, 95 Cal. Rptr. 3d 246 (Cal. Ct. App. 2009) (requiring production of internal data, chain of custody documentation, system access logs, audit logs, and testing results for voting machines to "aid in confirming or casting doubt upon the accuracy of the votes cast"); *see also* Declaration of Douglas W. Jones in Support of Motion for Summary Adjudication, *id.* (No. RG 04-192053).

328. *See* sources cited *supra* note 317.

oligopoly and the secrecy surrounding how most election equipment works—a conclusion that only underscores the need for a change in this market.

C. Open Testing and Audits

Being open to public scrutiny is necessary but not sufficient. The Act must additionally ensure that (1) routine systemwide security audits of election equipment and election outcomes, with audit procedures and audit results made public, are mandatory for any equipment essential to the correct functioning of an election; (2) research about security weaknesses in election equipment, even if unsolicited, are timely addressed by manufacturers and vendors; (3) researchers who conduct such research are legally protected from retaliation provided they follow safe harbor guidelines consistent with best practices in the security research community; (4) timely post-election audits, which provide statistical confirmation that a reported election outcome is correct, are mandatory in federal elections; and (5) provisions are made for empirical usability, accessibility, and security studies on any equipment essential to the correct functioning of an election, including research by independent third parties and academics.

Routine internal and external audits. Audits of election equipment should be conducted internally by equipment manufacturers themselves as well as at least one, and preferably multiple, groups of external experts independent of the equipment manufacturers and free of other conflicts of interest. The internal and external audit procedures should be publicly available, and audit results should be timely made public (after allowing a reasonable time for any discovered vulnerabilities to be fixed). Audits should be required before contracting and before deployment, and states must have the option to decline the contract without any penalty after carefully reviewing the audit results.

External security audits are a common practice for security-critical equipment in industry, even when the equipment in question is proprietary.[329] The basic underlying principle of external security audits can be expressed similarly to that of the legal adversarial system: a party whose whole interest is to play

329. *See, e.g.*, TRAIL OF BITS, https://www.trailofbits.com [https://perma.cc/K58T-QH5H].

the role of the adversary will be more likely to demonstrate the best possible adversarial strategy than a party whose interest is divided.[330] The Act should require full system access to be provided to auditors such that systems can be subjected to comprehensive adversarial-style scrutiny.[331]

Unsolicited security research. Researchers who have found security vulnerabilities in election technology and submitted reports to vendors and manufacturers are often treated with hostility or indifference. Voting machine companies have on multiple occasions threatened litigation in response to research reported to them in line with security best practices,[332] and they have ignored and denied serious problems of which they have been made aware, leaving known vulnerabilities unaddressed in machines actively used in American elections for as long as five or ten years.[333] Some companies have gone further and falsely claimed to have fixed such vulnerabilities.[334] This is problematic in several ways. Firstly, known serious security vulnerabilities are disregarded seemingly as a matter of course. Secondly, research into election security and reporting information to improve the security of election equipment should be encouraged—not chilled by threats of personal lawsuits against individual academics by large companies. Thirdly, current uncertainty in computer security law means that such threatened litigation is somewhat plausible and thus may be costly and time-consuming if undertaken.[335]

---

330. *See* Steven M. Bellovin et al., *Seeking the Source: Criminal Defendants' Constitutional Right to Source Code*, 17 OHIO ST. TECH. L.J. 1, 31 (2021) (elaborating this comparison and argument in a different context).

331. An established security audit technique known as "penetration testing" involves offering up one's systems to simulated adversarial scrutiny. *See What Is Penetration Testing?*, CLOUDFLARE, https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing [https://perma.cc/5E89-WVYK] ("[L]ike a bank hiring someone to dress as a burglar and try to break into their building and gain access to the vault. If the 'burglar' succeeds and gets into the bank or the vault, the bank will gain valuable information on how they need to tighten their security measures.").

332. *See* RUBIN, *supra* note 35, at 69; *Vulnerability Disclosure Guidelines*, HACKERONE (July 29, 2019), https://www.hackerone.com/disclosure-guidelines [https://perma.cc/9EL6-6BD3].

333. Newman, *supra* note 28; John Schwartz, *Computer Voting Is Open to Easy Fraud, Experts Say*, N.Y. TIMES (July 24, 2003), https://www.nytimes.com/2003/07/24/us/computer-voting-is-open-to-easy-fraud-experts-say.html [https://perma.cc/PJ8J-9EV3]; Calandrino et al., *supra* note 3.

334. JONES & SIMONS, *supra* note 3, at 161.

335. *See generally* KENDRA ALBERT & SUNOO PARK, A RESEARCHER'S GUIDE TO SOME LEGAL RISKS OF SECURITY RESEARCH (2020); Aaron Burstein et al., *Legal Issues Facing Election Officials in an Electronic-Voting World* (2007) (manuscript),

The Act should therefore introduce a safe harbor for researchers who report security vulnerabilities in election equipment, provided the reporting conforms with procedures to be defined and updated by the EAC.[336] These procedures should track industry best practices for vulnerability reporting, such as allowing adequate time for manufacturers to fix the reported vulnerabilities before disclosing the findings more widely. The safe harbor should also protect researchers' eventual publication of their findings after any required delays have elapsed, given that such transparency is important to promote security and given the public interest in keeping the public informed about election infrastructure security.

Finally, the Act should require election technology companies to timely fix reported vulnerabilities and communicate enough details about the fixes to the reporting researchers and the EAC so that the effectiveness of the fixes can be independently verified. The EAC should be able to initiate administrative action against vendors to enforce these requirements in the event of non-compliance and to allocate funding to state election offices to ensure that existing equipment known to have security vulnerabilities is fixed or replaced in a timely fashion.

Post-election audits. The Act should require audits to confirm the correctness of reported election outcomes, including *risk-limiting audits* done in consultation with statistical experts.[337] The audit process should be made open to public observation in accordance with applicable election observation protocols.[338]

Regular post-election audits and transparency around audit procedures are crucial for the checking component of the casting-counting-checking framework. Even the most carefully designed systems are susceptible to error from human mistakes or unexpected circumstances; so "[b]etter cybersecurity is not a substitute for effective auditing."[339] "Well-designed [and

---

https://www.law.berkeley.edu/files/Legal_Issues_Facing_Election_Officials.pdf [https://perma.cc/Y8R8-6PYQ].

336. *See* Daniel Etcovitch & Thyla van der Merwe, *Coming in from the Cold: A Safe Harbor from the CFAA and the DMCA §1201 for Security Researchers*, BERKMAN KLEIN CTR. RES. PUBL'N NO. 2018-4 (2018); Amit Elazari Bar On, *Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties*, *in* REWIRED: CYBERSECURITY GOVERNANCE 231 (Ryan Ellis & Vivek Mohan eds., 2019).

337. *See supra* Section II.E.

338. *See* CARTER CTR., *supra* note 80.

339. NAS REPORT, *supra* note 2, at 93.

properly performed] post-election tabulation audits can provide solid evidence to support the reported election outcome" when it is correct—and an opportunity to correct the outcome when it is not.[340] Recognizing these benefits, several states have already established statutory post-election audit requirements,[341] and multiple organizations that study election security and policy[342] as well as scientific experts[343] have advocated for mandatory post-election audits.

Usability, accessibility, and security studies. Rigorous studies of the usability and accessibility impacts of different kinds of election technologies,[344] the practical needs of voters from a wide range of backgrounds,[345] and the security implications of different election technologies[346] are essential for the casting and counting components of the casting-counting-checking framework.[347] These kinds of studies have tended to

340. *Post-Election Audits*, VERIFIED VOTING, https://verifiedvoting.org/audits [https://perma.cc/TAZ9-3SR4] [hereinafter *Verified Voting Post-Election Audits*]; *see also* Dartunorro Clark, *Cyber Ninjas, Company That Led Arizona GOP Election 'Audit,' Is Shutting Down*, NBC NEWS (Jan. 6, 2022), https://www.nbcnews.com/politics/politics-news/cyber-ninjas-company-led-arizona-gop-election-audit-shutting-down-n1287145 [https://perma.cc/3D7W-8GNP] (discussing a sham audit in Arizona in 2020, underscoring the importance of well-designed and properly performed audits).

341. *See 2022 NCSL Post-Election Audits*, *supra* note 30.

342. *See Post-Election Audits*, BRENNAN CTR. FOR JUST., https://www.brennancenter.org/issues/defend-our-elections/election-security/post-election-audits [https://perma.cc/CA5D-XYHJ]; *Verified Voting Post-Election Audits*, *supra* note 340.

343. *E.g.*, Appel & Stark, *supra* note 11 (making recommendations for RLA legislation).

344. *See* LAWRENCE NORDEN, BRENNAN CTR. FOR JUST., VOTING TECH. ASSESSMENT PROJECT, THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY, AND COST (2006), https://www.brennancenter.org/sites/default/files/press-releases/The%20Machinery%20of%20Democracy.pdf [https://perma.cc/HT4D-NWTY]; *Voting Systems Usability and Accessibility*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/programs-projects/voting-systems-usability-and-accessibility [https://perma.cc/BK6B-X4X2] [hereinafter *NIST on Accessible Voting*]; Stephen Knack & Martha Kropf, *Roll-Off at the Top of the Ballot: International Undervoting in American Presidential Elections*, 31 POL. & POL'Y 575 (2003); HENRY E. BRADY ET AL., COUNTING ALL THE VOTES: THE PERFORMANCE OF VOTING TECHNOLOGY IN THE UNITED STATES (2001); CALTECH/MIT VOTING TECH. PROJECT, VOTING: WHAT IS, WHAT COULD BE (2001).

345. *See NFB on Voting*, *supra* note 90; *NIST on Accessible Voting*, *supra* note 344.

346. *E.g.*, CALTECH/MIT VOTING TECH. PROJECT, *supra* note 344.

347. *See generally* NAS REPORT, *supra* note 2, at 75–77, 79 (discussing the importance of usable design of election technologies); *id.* at 118 (opining that "[a]lthough there are strong efforts by research groups and nonprofit organizations to gather data to inform election-related decisions and legislation, additional work

garner more attention and funding following prominent controversies, for example, the 2000 presidential election, but it is important to incentivize them as a more routine matter. HAVA provided some support for such studies;[348] and the new Act should build upon HAVA's provisions by (1) issuing funding on a regular (e.g., yearly) basis so that the attention these topics receive is more sustained and less dependent on political and media trends and (2) introducing incentives or requirements for voting technology vendors to make their technology widely available to researchers for the purpose of conducting independent usability, accessibility, and security evaluations, including empirical user studies.

D. Security Best Practices for All Election System Components

Most of the discussion so far has focused on the security of casting and counting, but other election system components—such as voter registration and systems for reporting results—are just as essential to the overall security of an election. Failures in these systems could undermine election integrity just as much as a failure in casting or counting. However, the security requirements of other election system components are much more similar to security requirements for other critical infrastructure.[349] As such, the Act should focus—and this Article focuses—more on security of casting and tallying, not because it is more important, but because it is more complex; and regarding other election system components, the legislation should ensure critical infrastructure and election security best practices are followed.[350] As also noted in prior work, state or

is needed" and that the federal government has a responsibility to sponsor research that protects the integrity of elections.); *id.* at 123.

348. *See NFB on Voting*, *supra* note 90; *NIST on Accessible Voting*, *supra* note 344.

349. Few critical infrastructure components have to interact directly with most voting-age citizens within a single day's timespan, with very limited opportunities for correcting mistakes, while being subject to unusually demanding security requirements—for example, ensuring access alongside eligibility verification in a nation lacking standardized proof of citizenship and ensuring ballot secrecy alongside convincing evidence of a correct outcome. *See, e.g.*, *Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors [https://perma.cc/UV9T-S4GY].

350. *See* CIS HANDBOOK, *supra* note 58; HKS CYBERSECURITY PLAYBOOK, *supra* note 58.

federal certification procedures and/or best practices documentation—for election equipment or for critical infrastructure in general—could facilitate efficient compliance.[351]

E. Reporting and Feedback Mechanisms

The Act should establish and maintain mechanisms for security experts, usability experts, accessibility experts, and election officials to communicate. Field experience with election technology should inform related regulation. But feedback from field experience to regulators is currently relatively weak due to a lack of established procedures as well as misaligned incentives. Under-resourced state election offices have a long list of higher priorities on and after Election Day than non-mandatory data gathering.

The Act should detail an investigation process where known vulnerabilities and incidents must be reported by election offices and vendors and then investigated by an independent governmental body, such as CISA, with allocated funding for such investigations.[352] As much information as possible from these investigations should be made public. Promisingly, the recently passed Cyber Incident Reporting for Critical Infrastructure Act of 2022[353] requires "cyber incident" reporting for review by CISA for all critical infrastructure. The Act should expand the scope of mandatory reporting to include vulnerability findings as well as incidents and provide detailed requirements related specifically to election security such as (1) expedited review, as well as corresponding funding and personnel allocation, when a pending election outcome may be impacted; (2) clarification of the scope of vendors that are subject

351. *See, e.g.*, NAS REPORT, *supra* note 2, at 8; Scott Shackelford et al., *Making Democracy Harder to Hack*, 50 U. MICH. J.L. REFORM 629 (2017). *But see* JONES & SIMONS, *supra* note 3, at 129–41 (discussing historical experience and potential pitfalls of federal standards and certification for election equipment); HALL, *supra* note 316, at 4–5 (discussing the same).

352. Somewhat like the Federal Aviation Administration's incident investigation process, which funds an office specialized in accident investigations and is separate from the airlines. *Office of Accident Investigation & Prevention*, FED. AVIATION ADMIN., https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/avp [https://perma.cc/78SP-SAAZ].

353. Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, 136 Stat. 49, 1038–59 (2022).

to reporting obligations—explicitly including vendors that specialize in election equipment or market their products for elections and exempting other upstream providers in the supply chain; and (3) special reporting requirements for independent security research findings and other testing performed outside of election conditions, which might not qualify as "incidents."

The Act should also establish regular workshops for interested experts to convene, become acquainted, discuss concerns in a confidential setting, and collaborate toward innovative solutions. In addition, it should establish more public conferences for industry, academic, and think tank research on the security, usability, and accessibility of election systems.

F. Voter Information and Education

The checking guarantee is not just about making sure that there are available means for the sufficiently educated and informed public to check that reported outcomes are correct; it is also about making sure the public is sufficiently educated and informed to adjudge election results credible (or not) based on the evidence available to them.[354] The Act should promote dissemination of such information to the public framed in simple and engaging language and incentivize supplementing schoolchildren's education about election systems and security in order to ensure that the next generation is better equipped to understand and reap the benefits of evidence-based elections.

G. Funding, Timing, and Agency Responsibility

None of the measures discussed thus far come for free. In an ideal world, "[r]ather than viewing the replacement of voting equipment as a generational occurrence, to take place only when the harsh light of public scrutiny forces alteration, legislative bodies [would] look upon the refurbishment of voting technology as an ongoing responsibility."[355] But pragmatically speaking, the harsh light of public scrutiny certainly helps—and now is

354. Interestingly, Germany takes the principle of public verifiability of elections even further: its Constitutional Court has held unconstitutional the use of voting machines (such as DREs) whose workings cannot be understood without specialist knowledge. *See* BVerfG, 2 BvC 3/07, Mar. 3, 2009, https://electionjudgments.org/api/files/15610577265627cak8qwuzp5.pdf [https://perma.cc/BM9K-HY4K].

355. Tokaji, *supra* note 140, at 1805.

another time, like the aftermath of the 2000 election, where threats to election integrity have gained national prominence and urgency conducive to funding allocations for election security and administration.

Together, the requirements of Sections V.A–V.F are substantial enough that they should be given to an agency to implement and enforce. The EAC and CISA would be natural choices, given their existing experience with election administration and cybersecurity, respectively.

When HAVA was passed, complications resulted from the president's delay in appointing EAC commissioners, Congress's failure to appropriate the authorized amount of funds for the first fiscal year, the tight timeframe for states to replace outdated voting systems, HAVA's lack of precise or binding technical standards for election equipment, and the EAC's lack of time to issue technical guidance before HAVA funds were spent.[356] The result has been described as "a massive deployment of faulty, flawed, and expensive equipment . . . [which] has led to security and integrity crises for which there are no clear-cut legal remedies."[357]

To avoid repeating these mistakes, the Act should include detailed technical mandates, provide for specific administrative enforcement, and allow more time for assessing and replacing equipment.[358] It should also allow the responsible agency to adjust this timeline in case of unexpected trouble with funding or other administration. Finally, the Act should regard the acquisition, maintenance, and replacement of election equipment as an ongoing process, not a one-off operation. Funding allocations and deadlines for election equipment maintenance and replacement should recur regularly,[359] taking into account the state of existing equipment and technical advances.

356. *See id.* at 1738–39; JONES & SIMONS, *supra* note 3, at 311–12.

357. JONES & SIMONS, *supra* note 3, at 312.

358. *See, e.g.*, Douglas W. Jones, *Some Comments on the Help America Vote Act of 2001* (Nov. 26, 2001), http://homepage.divms.uiowa.edu/~jones/voting/hr3295.html [https://perma.cc/D5BZ-ANWC] (proposing a detailed slower timeline for election equipment replacement in the context of HAVA).

359. *See* NAS REPORT, *supra* note 2, at 6 (recommending routine replacement).

VI. DISCUSSION OF POTENTIAL OBJECTIONS

This Part responds to some possible objections to the claim that election law should explicitly guarantee election system security, thus far laid out in this Article.

First, accessibility and security have sometimes been portrayed as values in inherent conflict with each other. In Section VI.A, I discuss access for voters with disabilities, how seeming tensions between security experts' recommendations and disabled voters' requirements have caused controversy, and my belief that the resulting debate has created a false dichotomy between values that are not only compatible but fundamentally aligned. Then in Section VI.B, I discuss a collection of recent cases that brought a variant "accessibility vs. security" narrative some limelight by challenging the 2020 presidential election based on claims that inadequate security measures facilitated widespread voter fraud. I explain how these unsuccessful cases differ importantly from the kinds of cases that would be successful under the theories articulated in Section IV.

Finally, reports of widespread mistrust and misinformation regarding election integrity in recent years may have led some to the disillusioned view that technical security measures are inadequate or futile to address the modern problem of public trust in elections. Put differently, if it appears that government-backed security measures will be distrusted by a significant part of the population for political reasons more than technical reasons, then it may seem that technical security measures are the wrong answer. In Section VI.C, I discuss why I believe technical improvements to election security are an important part of improving trust in elections, even though technical improvements alone will not suffice.

A. The False Dichotomy of "Accessibility vs. Security"

"We must debunk the myth that we have to choose between accessible voting and verifiable voting. Democracy requires . . . both."[360]

360. *ACLU and Disability Law Center Applaud Secretary Galvin's Decision on New Voting Technology*, ACLU (Mar. 5, 2007), https://www.aclu.org/press-releases/aclu-massachusetts-and-disability-law-center-applaud-state-approval-new-voting [https://perma.cc/B34R-MZ2P].

Significant pushback on paper ballot requirements relates to accessibility and disability. The pushback predates HAVA; it originated at a time when those who could not mark a paper ballot by hand were left to tell their choices to another person of their choice and hope that their ballot got cast and counted, a time when the security risks of electronic voting machines were considerably less understood than today.[361]

HAVA led to important efforts to improve the accessibility of voting, which have enabled some disabled voters to cast their votes "independently as never before."[362] However, much progress remains to be made; research done years after HAVA noted that "many of the [machines adopted to meet HAVA's accessibility requirements that are] in use today do not fulfill the promise of accessibility for the majority of voters with disabilities."[363]

HAVA's accessibility and equipment upgrade requirements led to the widespread adoption of DRE machines that were later established to have serious security flaws. The subsequent push for voter-verifiable paper records has led to a heated debate that sometimes appears to pit security against accessibility in a counterproductive false dichotomy. Accessibility is essential to secure systems; it is not acceptable to exclude necessary users from effectively accessing the system. As noted in Part I, accessibility for all eligible voters is core to the availability principle.[364] Security is also essential to accessible systems; it is not an acceptable solution to provide broken but easy-to-use technologies to voters with disabilities.

Yet even works that acknowledge the importance of both access and security tend to focus with more expertise on one side (including this Article)—an unsurprising, though frustrating, consequence of a specialized issue that intersects two complex fields of expertise. Discourse based on accessibility expertise often describes accessibility benefits (or harms) of certain election technologies while seeming to implicitly assume that those technologies will function correctly as advertised; discourse based on security expertise often describes the security benefits (or harms) of certain election technologies

361. *See* RUNYAN, *supra* note 99; sources cited *supra* note 192.

362. *NFB on Voting*, *supra* note 90.

363. RUNYAN, *supra* note 99, at 8.

364. Indeed, if this were not the case, then it would be easy to build secure systems by preventing all access and providing no useful functionality.

while seeming to implicitly assume that those technologies can be used by everyone who needs to.

Further, given the inescapable political undercurrents of the topic, "attacking DREs for bad security was considered by some disabilities advocates as an attack on the access movement."[365] It is possible that, similarly, attacking security recommendations for inadequate accessibility provisions could be perceived as politically motivated opposition and brushed aside by some as based on a lack of technological understanding. The politicization of the issues has likely heightened acrimony and a feeling of two entrenched "sides" talking past each other; yet on both sides, scholars and practitioners of accessible technologies and security are concerned about objective technological problems based on a scientific approach, whether in the form of empirical usability studies or research demonstrating security vulnerabilities. A more collaborative conversation and mutual understanding should be possible between these communities. Promisingly, there has been progress over the years toward both types of experts "accept[ing] the notion that access and security are both important and not incompatible . . . ."[366]

The debate over paperless electronic voting machines seems sometimes to be characterized as a question of fine-tuning where to strike the balance between the two competing values of security and accessibility. In theory, it could be the case that we are truly faced with a choice between two alternative technologies whose main difference is that one is slightly more accessible but slightly less secure than the other; such a situation would indeed call for a nuanced policy judgment that might come out either way depending on the fact-specific balancing of priorities.

But in the debates over paperless electronic voting machines, unfortunately, this is not the kind of choice with which we are faced. The accessibility benefits of such machines can be great, but those same benefits could be entirely undermined if the security of the machines is very easily compromised. In other words, the issue in such cases is not whether this amount of accessibility benefit is worth trading off against that amount of security harm, but whether the seeming benefit is actually undermined by serious additional risks.

365. RUNYAN, *supra* note 99, at 8.
366. *Id.* at 9.

The problem of designing secure and accessible voting technology is a complex and challenging one, and there remains much improvement to be made. However, the two goals are fundamentally aligned—security is not useful without accessibility and vice versa—so debating which to prioritize over the other is a mistaken framing. Rather, it is important to foster innovation and collaboration between security and accessibility experts to develop voting technologies with improvements in both accessibility and security at once.[367] Using purely hand-marked paper ballots is not an acceptable solution, as they are unusable by several percent of the electorate; and paperless electronic voting machines are not an acceptable solution either, as they provide no reliable evidence trail to confirm or refute machine-reported election results.

B. Lawsuits Challenging the 2020 Presidential Election

A collection of lawsuits before and after the 2020 presidential election challenged the election results and administration, bringing a variant "accessibility vs. security" narrative some limelight. These lawsuits claimed that inadequate security measures facilitated widespread voter fraud and thereby diluted the votes of non-fraudulent voters.[368] For example, plaintiffs in Pennsylvania challenged the state's provision of unmonitored ballot drop boxes, alleging that they allowed for significant fraud.[369] Plaintiffs in Minnesota challenged the counting of ballots postmarked by Election Day and received up to a week afterward, arguing that the "persons watching the elongated ballot-counting" would somehow "face strong incentives" to cast additional late ballots even if they had

367. Ballot-marking devices (BMDs) are an example of a technology that makes progress towards this, although there remain notable concerns about the technology, and it needs to be better tested. *See* Appel et al., *supra* note 103. Improving BMDs or coming up with innovative alternatives to BMDs, and finding new ways to make BMD-marked ballots indistinguishable from hand-marked ballots, could be valuable future research directions. *See id.*

368. *See* Stephanopoulos, *supra* note 263, at 1183–88 (providing a detailed summary of the lawsuits claiming vote dilution by fraud facilitation); *COVID-Related Election Litigation Tracker*, STANFORD-MIT HEALTHY ELECTIONS PROJECT, https://healthyelections-case-tracker.stanford.edu [https://perma.cc/6N4S-HKLR] (a searchable online database of election litigation during the 2020 election season).

369. Donald J. Trump for President, Inc. v. Boockvar, 493 F. Supp. 3d 331, 359–64 (W.D. Pa. 2020).

already voted.[370] Plaintiffs in Illinois challenged the state's making Election Day a holiday for state workers, arguing that "state workers, who primarily vote Democrat" would then constitute "an army of workers" who "could show up to the polls on election day" and cast fraudulent ballots.[371]

While none of these cases were ultimately successful, and while the claims' structures differed notably from traditional vote dilution claims,[372] "most courts that have confronted claims of vote dilution through fraud facilitation have treated them as legitimate grounds for relief."[373] The reasoning behind their dismissals has generally been lack of standing or an application of *Anderson-Burdick* finding the burden—often deemed minimal—of the challenged practice to be justified by state interests.

A natural question then arises: Would recognition of the theory of the constitutional right to vote set out in Part IV be inconsistent with the outcomes of the cases challenging 2020 election practices? The answer is no; the 2020 cases are easily distinguishable from the kind of case that would be successful under the theory of Part IV, as described next, and "it should be possible to mitigate the risk of bad faith litigants hijacking [legal theories that recognize substantiated claims of fraud] by carefully limiting standing, liability, and relief."[374] First, the 2020 cases made claims that were not substantiated in evidence—that is, they did not (and probably could not) prove the alleged causal link between the challenged election practices and a greatly increased ease of perpetrating fraud.[375] Secondly, even if the plaintiffs *were* to prove that causal link, most of the kinds of fraud alleged were relatively small scale and would thus amount to a relatively small burden or risk, meaning relief would be very limited if available at all. Thirdly, inappropriate

370. Carson v. Simon, 494 F. Supp. 3d 589, 602 n.12 (D. Minn. 2020), *rev'd on other grounds*, 978 F.3d 1051 (8th Cir. 2020).

371. Cook Cty. Republican Party v. Pritzker, 487 F. Supp. 3d 705, 719 (N.D. Ill. 2020).

372. *See supra* Section IV.C.

373. Stephanopoulos, *supra* note 263, at 1181.

374. *Id.* at 15–16 ("In a polarized area, th[e] unbroken wall of opposition [to the 2020 election fraud claims] is impressive. Liberal and conservative judges, Obama and Trump appointees—they all refused to rule in favor of groundless claims.").

375. Sometimes, those concerned about the 2020 election practices do not stop at claiming, as in Part III's theory, that there is a problem because the election system makes fraud too easy; they further make substantive and baseless claims that, therefore, massive fraud actually happened. *See supra* Section II.F.

kinds of relief requested in some of the 2020 cases (e.g., de-certifying election results) are unsupported by Part III's theories (of constitutional voting-rights challenges to insecure election infrastructure) no matter how egregiously insecure an election practice is at issue.[376]

Table 1 summarizes several factors, including the above, that distinguish between the types of meritless claims made in the 2020 election litigation and hypothetical legitimate challenges to insecure election infrastructure under the theories of Part III. Some of the 2020 litigation shares certain features of legitimate challenges, as indicated in orange italics. However, even such litigation—with many shared features—would be clearly distinguishable from a legitimate challenge to insecure election systems, based on the many other middle-column entries in red.

Table 1. Distinguishing features of legitimate challenges to insecure election systems

	2020 election litigation	**Legitimate challenges to insecure election infrastructure**
Timing (relative to election)	· *Prospective* · Last-minute · Retrospective	· Prospective only
Basis for claim	· *Vulnerabilities in election infrastructure* · Actual election fraud	· Vulnerabilities in election infrastructure

376. *See supra* Section III.D.

Scale of potential harm (if allegations true)	· Likely very localized · If large-scale, would likely be detectable	· Could enable large-scale fraud with low likelihood of detection
Supporting evidence	· Unfounded speculation	· Reputable research with verifiable scientific claims
Relief requested (injunctive)	· *Concrete changes to election infrastructure or procedures to mitigate or resolve the alleged problem* · De-certification of results · Judicial re-certification of different results	· Concrete changes to election infrastructure or procedures to mitigate or resolve the alleged problem
Disposition	· Consistently rejected	· Relief should be granted in appropriate cases

However, it bears note that the standing analyses in some, but not all, of the 2020 cases could preclude legitimate claims based on serious vulnerabilities in election infrastructure because of their emphasis on particularized harm requiring a showing that plaintiffs' votes more than other voters' votes would be "diluted." In cases challenging systemic practices that may cause severe unreliability in the election results in a way that is indiscriminate or unpredictable between voters, I believe that the particularized harm requirement must be adapted in order to effectively protect the fundamental right to vote, and courts have already shown a willingness to recognize standing in such cases in Georgia and elsewhere.[377]

Another concern related to the 2020 lawsuits is about the negative impacts of measures that, in the name of preventing fraud, make it more difficult for many eligible voters to vote—especially given evidence that such fraud is "very rare in modern

377. *See* cases cited *supra* note 10; Stewart v. Blackwell, 444 F.3d 843 (6th Cir. 2006).

American politics (at least at any significant scale)."[378] Would the theory in Part IV just give "another legal weapon"[379] to those who invoke fraud, speculatively or without substantiation, to push for measures that would make voting harder for many eligible voters? Again, I believe not. Courts rightly recognize such systemic insecurity in elections as *potential* grounds for relief but have consistently denied relief upon further legal analysis in the factual contexts in which such fraud-based cases were brought. Indeed, courts have already shown themselves to be more receptive to constitutional challenges to unreliable voting methods than to fraud-driven challenges in realistic, factual contexts, sometimes granting relief for the former while consistently denying relief for the latter, even while recognizing both as legitimate grounds for relief in theory.

Of course, even if courts continue consistently rejecting unfounded claims as they have so far, and no matter how efficient they are, the period of pendency of a meritless suit can be deeply fraught if it appears that an election outcome may be at stake. Yet the prevalence of unfounded claims should not be permitted to obscure the significance of serious concerns founded on established scientific evidence—especially in a context where meritless claims, though recently numerous, are easily distinguished from legitimate ones, and where courts have more than demonstrated their readiness to distinguish them. A focus on prospective challenges, as I suggest, as well as existing doctrines wherein courts will not interfere with imminent or ongoing elections,[380] will further aid efficient dismissal of those suits that appear to implicate impending election outcomes.

C. Improving Public Trust in Elections Needs Both Technical and Political Measures

It may seem that the problem with recent contested elections is political, rather than technical, in nature. A possible cynical conclusion from this perspective would be that, regardless of any improved technical security measures and

378. Stephanopoulos, *supra* note 263, at 1181; *see also Debunking the Voter Fraud Myth*, BRENNAN CTR. FOR JUST., https://www.brennancenter.org/sites/default/files/analysis/Briefing_Memo_Debunking_Voter_Fraud_Myth.pdf [https://perma.cc/AZ9C-6VX5].

379. Stephanopoulos, *supra* note 263, at 1181.

380. *See* cases cited *supra* note 277.

evidence about the correctness of election outcomes, politically motivated mistrust of elections will persist.

The problem of bolstering confidence in elections is a highly political one, but it has technical aspects too. Legislators and policymakers have an obligation to promote the development and adoption of secure election technologies and provide convincing evidence of correct election conduct as a necessary but insufficient part of a broader policy agenda to promote trust in elections. The "anything technical will be questioned" argument could equally be applied to dismiss most of the incremental advances in election conduct since the Chartist proposal for using secret ballots and voting machines in the 1830s, yet in aggregate, the result has been a huge improvement in election convenience and security. Furthermore, the harmful political rhetoric that is undermining confidence in American elections and democracy[381] will only be exacerbated by a continued failure to take technical aspects of election security seriously—and could even be rendered largely irrelevant if election system insecurities so worsen as to hand over control of U.S. elections to foreign adversaries.

While recognizing that neither a purely technical nor a purely political solution will suffice to address the problem of public trust in elections, and that the current decline of confidence in American elections and democracy is indeed highly political in nature, this Article focuses primarily on technical aspects of the problem.

CONCLUSION

Confidence in U.S. elections is on the decline. Lawmakers, politicians, the media, and the broader public are expressing concern about election systems' accuracy, reliability, accessibility, resilience to fraud, and resilience to domestic or foreign manipulation. The questions underlying all these concerns include: *Are our elections secure enough? How can we be sure? And if they are not, what can we do about it?* The stakes are high: "If the challenges currently facing our election systems are ignored, we risk an erosion of confidence in our elections

381. *See, e.g.*, Michael J. Klarman, *The Degradation of American Democracy — And the Court*, 134 HARV. L. REV. 1, 42–45 (2020).

system and in the integrity of our election processes,"[382] signs of which we are already seeing today.

These pressing challenges call for swift adaptation and innovation in both election law and election technology. The Constitution provides a valuable starting point. Large-scale election infrastructure insecurity poses a threat to the fundamental right to vote that constitutional jurisprudence cannot ignore. But ultimately, constitutional litigation is a necessary but insufficient stopgap pending the urgent passage of modern, robust, and comprehensive election security legislation. Election law needs to adopt new approaches to transform an entrenched and resistant election equipment market, to explicitly recognize actionable harms arising from election system insecurity and associated risks, and to provide election administrators additional resources to protect their systems—and thereby to secure American election infrastructure and provide the public with convincing evidence that elections are run with integrity.

382. NAS REPORT, *supra* note 2, at 122.