VIRGINIA LAW REVIEW ONLINE

VOLUME 105 FEBRUARY 2019 67-83

ESSAY

HACKING THE RIGHT TO VOTE

*Jacob Rush**

Most Americans believe the right to vote is one of the most important constitutional rights.[1] Moreover, eight out of ten Americans are concerned the country's voting system is vulnerable to hackers.[2] Although new voting technology has been implemented across the country, it largely enables, rather than prevents, hacking, causing "frightening vulnerabilities" for election administration.[3] It seems that "America's most ancient civilian office, the local election clerk, has become saddled with new and alien responsibilities tantamount to a military contractor."[4]

* Second-year law student, University of Virginia School of Law. The ideas below are inspired by Professor Michael Gilbert, who taught me dozens of things I didn't know I wanted–and needed–to know. Thanks also to Chinmaya Sharma, who encouraged me to write this paper, gave me incisive feedback on earlier drafts, and never let me lose my voice; and my partner, Ali Block, for always reminding me that there are more important things in the world than papers. Thanks finally to my grandma, Mary Lee Haug, who is my first teacher, last editor, and the best wordsmith I know.

[1] Brian Pinaire et al., Barred from the Vote: Public Attitudes Toward the Disenfranchisement of Felons, 30 Fordham Urb. L.J. 1519, 1533–34 (2002) (finding that 93.2% of survey respondents believe that the right to vote is either the most important or one of the most important rights in a democracy).

[2] Billy Morgan, New Survey Reveals Concerns About the Security of the Nation's Voting System Ahead of the Midterm Election, U. of Chi. Harris Sch. of Pub. Pol'y (Oct. 10, 2018), [https://perma.cc/N4CG-MXQ2].

[3] Benjamin Wofford, The Hacking Threat to the Midterms Is Huge. And Technology Won't Protect Us., Vox (Oct. 25, 2018, 5:00 AM), [https://perma.cc/3XX4-VD2G].

[4] Id.; see also Alejandro de la Garza, Should You Be Afraid of Election Hacking? Here's What Experts Say, Time (Oct. 25, 2018), [https://perma.cc/E7HM-A76Y] (explaining the

Hacking presents a novel threat to elections and may have far-reaching implications on the right to vote.

Part I describes the current state of election technology and the hurdles preventing improvements. Part II addresses Russia's cyberattacks in the 2016 elections. It highlights the unprecedented risk hacking poses to the right to vote and suggests that courts must intervene. Part III reviews recent litigation to suggest that vulnerable voting machines violate the right to have one's vote counted accurately, which reimagines traditional right-to-vote jurisprudence in the context of hacking. Finally, Part IV posits that hacks that burden voter access, increase voter frustration, and foil voter participation are more likely, just as dangerous, yet less responsive to right-to-vote jurisprudence than hacks manipulating vote tabulations.

I. THE PROBLEM WITH VOTING TECHNOLOGY: FEDERALISM, FUNDING, AND INDUSTRY

Voting technology matters so much because elections are so often so close. Accurate machines ensure that the electoral process both selects true winners and convinces losers to accept unfavorable results.[5] The constitutional right to vote accordingly guarantees that each voter has about the same opportunity to have his or her vote counted, by requiring that counting methods (e.g., voting machines) distribute counting errors roughly equally. This is the promise and peril of *Bush v. Gore*.[6] Problems with voting technology, where some legally valid votes may not be counted properly, which produces high residual vote rates, risk undermining the fundamental right to vote and the public's confidence that the will of the people has been freely and fairly expressed.[7]

---

vulnerability of elections in view of the unprecedented nature of the threat, including equipment hacks and misinformation campaigns).

[5] Richard L. Hasen, The Voting Wars 8-10 (2012) (emphasizing the importance of public confidence in election results, and of widespread election reform in securing that confidence, in the wake of Bush v. Gore).

[6] Bush v. Gore, 531 U.S. 98, 104–05 (2000) ("The right to vote is protected in more than the initial allocation of the franchise. Equal protection applies as well to the manner of its exercise. Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another.").

[7] The nation lost approximately between 4 million and 6 million votes in the 2000 presidential election. The Caltech/MIT Voting Tech. Project, Voting: What Is What Could Be 8–9 (2001) [hereinafter Voting Technology Project]. Using residual votes and lost votes from the past four presidential elections, 1.5 million presidential votes and 3.5 million votes for governor and senator are lost each election because of problems with voting equipment. Id.

Despite the stakes, there are three roadblocks to better voting machines.[8] First, federalism. According to the constitution's text and the gloss of history and tradition, states have wide discretion in election administration.[9] They run federal elections subject only to Congress's authority, exercised occasionally, [10] to "at any time by Law make or alter such regulations."[11] States also have plenary power over the time, place, and manner of local elections, subject to the restriction that they not *over*burden the right to vote.[12] Accordingly, federal legislators fiercely resist anything resembling federal interference with state autonomy.[13]

Second, funding. Although many election officials say that modernizing voting technology is an important concern,[14] there are scant resources available to them to address it.[15] Modernization, to be sure, is not cheap. South Carolina estimates that it will cost $40 million to replace

[8] Despite opportunities to improve election technology, hardware and software products have barely advanced in the last decade. See Penn Wharton Pub. Pol'y Initiative, The Business of Voting 19 (2017) [hereinafter Business of Voting]. See generally The Presidential Commission on Election Admin., The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration (2014) [hereinafter Election Administration Commission] (explaining the problems with existing voting technology and recommending updates).

[9] U.S. Const. art. 1, § 4, cl. 1.

[10] Congress did not pass a law regulating federal election administration until 1842. Ex Parte Yarbrough, 110 U.S. 651, 660 (1884); see also An Act For The Apportionment of Representatives Among the Several States According to the Sixth Census, ch. 47, 5 Stat. 491 (1842). Congress passed comprehensive statutes in 1870 and 1871 in order to enforce the Fifteenth Amendment. See Force Act of 1870, ch. 114, 16 Stat. 140 (1870); Force Act of 1871, ch. 99, 16 Stat. 433 (1871) (amending the Force Act of 1870); Ku Klux Klan Act, ch. 22, 17 Stat. 13 (1871). Between 1957 and 1982 Congress passed several laws protecting the right to vote free of intimidation and arbitrary or capricious factors. See, e.g., 42 U.S.C. §§ 1971 et seq. (2012).

[11] U.S. Const. art. 1, § 4, cl. 1.

[12] See U.S. Const. art. 1, § 4, cl. 1; Wesberry v. Sanders, 376 U.S. 1, 6–7 (1964); Tashjian v. Republican Party of Conn., 479 U.S. 208, 217 (1986) ("The power to regulate the time, place, and manner of elections does not justify, without more, the abridgement of fundamental rights, such as the right to vote." (citation to *Wesberry* omitted)).

[13] Wofford, supra note 4.

[14] See Election Administration Commission, supra note 8, at 11 & n.10 (finding that, in a nationwide survey of election officials, twenty-four percent of respondents said that "voting technology and voting machine capacity" need improvement or update—the highest percentage of any category in the survey).

[15] Id. at 10 (explaining that the most common complaint of election administrators is a lack of resources and that election administrators characterize themselves as "the least powerful lobby in the state legislatures").

its voting machines—$39 million more than its legislature allocated in 2017.[16]

Finally, industry. The roughly $300 million market[17] for voting technology is problematic. The industry is small but politically well connected, with especially strong ties to the Republican Party.[18] It is mostly regulated at the state level.[19] Customers are often locked into long-term contracts and face high switching costs, destroying industry incentives to innovate.[20] Certifying new technology takes years.[21] Equipment designs, hardware, and software are usually proprietary.[22] Companies thus fight in court to prevent prying eyes when challenged. John Kerry lost a battle in 2004 to access the source code behind voting machines in Ohio.[23] So too did a 2006 candidate for Florida's 13th Congressional District, who alleged that machines in one county erroneously registered 18,000 "no" votes in her race.[24] Moreover, the industry is composed of only three hardware companies that manufacture over eighty percent of machines and, in contrast, a large number of tiny third-party software vendors.[25] And of the few industry-wide changes made after *Bush* in 2000, some actually undermined opportunities to innovate and improve the voting experience.[26]

Congress passed the Help America Vote Act ("HAVA") in 2002 in response to *Bush*.[27] HAVA authorized $3.65 billion in payments to states to improve voting technology, and appropriated $3.28 billion of that amount between 2003 and 2010.[28] States used funds to purchase new machines, often direct-recording electronic ("DRE") or optical-scan

[16] Michael Wines, Wary of Hackers, States Move to Upgrade Voting Systems, N.Y. Times (Oct. 14, 2017), [https://perma.cc/4A96-YC9H].

[17] See Business of Voting, supra note 8, at 23.

[18] Kim Zetter, The Crisis of Election Security, N.Y. Times (Sept. 26, 2018), [https://perma.cc/Z6DW-JH2Q].

[19] Business of Voting, supra note 8, at 30.

[20] Id. at 32–36.

[21] Id. at 38.

[22] Id. at 42.

[23] Zetter, supra note 18.

[24] See H.R. Rep. No. 110-528, at 2–3 (2008).

[25] Business of Voting, supra note 8, at 14–15, 18–19, 54.

[26] See generally Stephen Ansolabehere & Ronald Rivest, Voting Equipment and Ballots (2013), [https://perma.cc/PX57-ZSU9].

[27] Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (2002) (prior to 2010, 2018 amendments).

[28] Arthur L. Burris & Eric A. Fischer, Cong. Res. Serv., The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election, at Summary (2016).

machines.[29] DREs read digital ballots. Optical-scanners read paper ballots. Both machines store votes on memory cards. Optical-scanners keep digital images of the paper ballots they read, which can provide an audit trail. DREs can, but do not always, print paper images that voters can review, although their scrolls could conceivably be hacked to print voters' choices correctly while recording different choices on the memory card.[30] Whereas in 2000 just nine percent of voting precincts were using DREs, after HAVA was passed the number of precincts using DREs increased to sixty-seven percent, despite the risk of hacking.[31]

Whatever gains were realized in the early 2000s have been all but lost. Forty-one states still use machines that are at least ten years old,[32] which creates a higher risk of failure and predictable vulnerabilities. Thirteen states still use machines that do not provide paper trails.[33] Some states report scavenging for new parts on eBay.[34] Forty-three states and the District of Columbia use voting machines that are no longer manufactured.[35] In 2018, Congress provided $380 million more in grants to states to improve federal election administration.[36] Yet these appropriations are entirely insufficient to replace voting machines, which are "reaching the end of their natural life cycle."[37] It would cost $2 per voter *per year*, [38] or over $270 million annually based on recent presidential-election turnout rates,[39] to upgrade and properly maintain voting machines across more than 10,000 "hyperdecentralized" election jurisdictions.[40]

---

[29] See Business of Voting, supra note 8, at 11, 13, 19, 55.

[30] Zetter, supra note 18.

[31] Id.

[32] Lawrence Norden & Wilfred U. Codrington III, America's Voting Machines at Risk—An Update, Brennan Ctr. for Just. (Mar. 8, 2018), [https://perma.cc/Z3AH-YJZW].

[33] Id.

[34] Id.

[35] Lawrence Norden & Wilfred U. Codrington III, Brennan Ctr. for Just., America's Voting Machines at Risk 15–16 (2015), [https://perma.cc/7XZL-9UK4].

[36] Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, Div. E, Tit. V (2018); see also U.S. Election Assistance Commission, 2018 HAVA Election Security Funds, [https://perma.cc/75VV-G6NW] (last visited Jan. 14, 2019).

[37] Election Administration Commission, supra note 8, at 63.

[38] See Voting Technology Project, supra note 7, at 53.

[39] Federal Election Commission, Official 2016 Presidential General Election Results 7 (Jan. 30, 2017), [https://perma.cc/MJ3V-VZ3H] (showing that 136,669,237 votes were cast in 2016 for president).

[40] Hasen, supra note 5, at 8; Election Administration at State and Local Levels, Nat'l Conf. of St. Legislatures (June 15, 2016), [https://perma.cc/R5P9-QNVN].

The rapid shift to new voting technology in the wake of *Bush*, although well-intended, was poorly implemented. Coupled with inadequate maintenance and industry standstill, it created the conditions in which the hacks that now imperil the right to vote could occur. Indeed, software vendors, in at least one instance, let known security issues persist for eleven years.[41]

The strings attached to HAVA's grants[42] arguably hurt election security more than they helped. First, states had to consolidate voter registration databases previously maintained at the county level.[43] That created a one-stop shop for breaches. Second, the Act's strict (albeit necessary) voting standards limited the kinds of voting machines states could buy with HAVA funds.[44] That lead to widespread adoption of electronic voting technology,[45] which in turn created incentives for private companies to rush to market with untested machines to take advantage of the windfall of cash and to sell states products that were not needed, such as e-pollbooks, which election officials often use to check-in voters on Election Day. Finally, states had to implement changes before the 2004 federal election,[46] leaving no time for risk assessment, debugging, or testing. The speedy move to technology, without a plan or the funds to upgrade software and hardware regularly, was a solution in search of a problem: hackable voting machines.[47]

---

[41] Wofford, supra note 3; see also Sue Halpern, Election-Hacking Lessons From the 2018 Def Con Hackers Conference, New Yorker (Aug. 23, 2018), [https://perma.cc/9JXB-JQJ5] (explaining that, despite extensively documented vulnerability to hacks, the AccuVote-TSX is still in use in eighteen states).

[42] Help America Vote Act of 2002, Pub. L. No. 107-252, §§ 101–02, 253, 301, 303–04, 116 Stat. 1666 (2002) (prior to 2010, 2018 amendments).

[43] Id. at § 303.

[44] Id. at §§ 102, 301; see also Burris, supra note 28, at 5 ("Under HAVA, systems used in federal elections must provide for error correction by voters, accessibility for persons with disabilities, manual auditing, alternative languages, and error-rate standards. Systems must also maintain voter privacy and ballot confidentiality, and states must adopt uniform standards for what constitutes a vote on each system.").

[45] Election Assistance Commission, The 2014 EAC Election Administration and Voting Survey Comprehensive Report 14, 264–65 tbl. 42 (June 30, 2015), [https://perma.cc/AQG5-8JMQ] (finding that in 2014 the DRE without a voter audit trail was the most widely deployed technology across the states and that DREs overall made up nearly seventy percent of all voting machines).

[46] Help America Vote Act of 2002, Pub. L. No. 107-252, § 102(a)(3), 116 Stat. 1666 (2002) (prior to 2010, 2018 amendments).

[47] It also ignored one of the central lessons of *Bush*: Volusia County. There, partly due to a faulty memory card and computer glitch, Al Gore lost 16,000 votes in a matter of minutes while the Socialist candidate gained 10,000. See Dana Milbank, Tragicomedy of Errors Fuels

II. HACKING AND THE RIGHT TO VOTE

The last presidential election put election hacking on the map, although election officials have been aware of the risk of hacking for decades.[48] Russia's attacks practically compel the conclusion that problems with election technology are not just "political questions" for the "political branches,"[49] but rights-based threats that demand the attention of courts. Where the political system fails to adequately protect election integrity and the right to vote, courts must fill the vacuum.

Russia's attacks were, indeed, unparalleled in nature and scope.[50] Russian hackers targeted election infrastructure in twenty-one states with sophisticated cyberattacks.[51] They successfully breached voter registration rolls in Illinois,[52] stole the username and password of an election official in Arizona,[53] and infiltrated an unnamed private

Volusia Recount, Wash. Post (Nov. 12, 2000), [https://perma.cc/3QYN-3XLM]; but see Zetter, supra note 18 (questioning whether the faulty memory card caused the mishap).

[48] Paul Krugman, Hack the Vote, N.Y. Times (Dec. 2, 2003), [https://perma.cc/T7XJ-MR2H]. There was also a 1969 front-page article in *Los Angeles Times* describing a "war games" exercise to determine if computerized punch-card readers could be rigged, which provided "a chilling look at the state of computer art and the implications it holds for future elections," when the "offensive" team, tasked with finding ways to rig the election machines, won all six trials by successfully infiltrating the machines without being detected by the countermeasures implemented by their opponents. See Richard Bergholz, How Elections Can Be Rigged Via Computers, L.A. Times, July 8, 1969, at 1, 24.

[49] See Nixon v. United States, 506 U.S. 224, 228 (1993) ("A controversy is nonjusticiable––i.e., involves a political question—where there is a 'textually demonstrable constitutional commitment of the issue to a coordinate political department; or a lack of judicially discoverable and manageable standards for resolving it . . . .'"); see also Baker v. Carr, 369 U.S. 186, 210–11 (1962) (discussing the nature of a "political question").

[50] Although the intelligence community insists no results were altered, there has not been a full examination of all the evidence. "Intelligence assessments are based on signals intelligence—spying on Russian communications and computers for chatter or indicating that they altered votes—not on a forensic examination of voting machines and election networks." Zetter, supra note 18.

[51] Russian Interference in the 2016 U.S. Elections: Hearing Before the S. Select Comm. on Intelligence, 115th Cong. 5 (2017) (statement of Samuel Liles, Acting Dir. of the Cyber Div., Office of Intelligence and Analysis, Dep't of Homeland Sec.); see also Nat'l Intelligence Council, Office of the Dir. of Nat'l Intelligence, Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections 3 (2017), [https://perma.cc/S3BQ-UUCE].

[52] Nicole Perlroth et al., Russian Election Hacking Efforts, Wider than Previously Known, Draws Little Scrutiny, N.Y. Times (Sep. 1, 2017), [https://perma.cc/VP4R-E3MJ]; see also Matthew Cole et al., Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election, Intercept (June 5, 2017, 3:44 PM), [https://perma.cc/9ZMA-GV7R] (reporting on leaked NSA document detailing Russian hacking).

[53] Miles Parks, Will Your Vote Be Vulnerable on Election Day?, NPR (May 8, 2018, 5:00 AM), [https://perma.cc/RS7H-58PE].

company.[54] Russian hackers also sent emails to 122 email addresses associated with named local governmental organizations and election officials containing malicious code[55] and accessed county election websites in Georgia, Iowa, and Florida.[56] The era of local administrative control over voting technology is over. Russia's hacks changed the narrative.

The right to vote, which is implicated by voting technology in ways unforeseeable even a decade ago, is a fundamental constitutional right.[57] At bottom, the idea is that "[t]he conception of political equality from the Declaration of Independence, to Lincoln's Gettysburg Address, to the Fifteenth, Seventeenth, and Nineteenth Amendments can mean only one thing—one person, one vote."[58] The right adapts to the times, precluding first-generation infringements (restrictions on an individual's ability to cast a ballot) as well as second-generation infringements (efforts to dilute the effectiveness of one's vote).[59] This jurisprudence culminated in *Bush v. Gore,* which applied the right to vote to election administration specifically, holding that counting votes by methods or means with similar levels of accuracy, or probabilities of inaccuracy, is part and parcel of the right to vote.[60] As a result, when states rapidly modernized their

[54] Cole et al., supra note 52.

[55] Id.

[56] Indictment at 26, United States v. Netyksho, No. 18-cr-00215 (D.D.C. July 13, 2018).

[57] The Supreme Court has pointed to a number of constitutional provisions to establish the fundamental right to vote. See, e.g., Bush v. Gore, 531 U.S. 98, 104–05 (2000) (once the state legislature vests the right to vote in its people, equal protection applies to the manner of its exercise); Anderson v. Celebrezze, 460 U.S. 780, 787–88 (1983) (the right to vote is protected by the Due Process Clause of the Fourteenth Amendment, which embraces the First Amendment); Reynolds v. Sims, 377 U.S. 533, 560–61 (1964) (the right to vote in state elections is protected by the Equal Protection Clause of the Fourteenth Amendment); Gray v. Sanders, 372 U.S. 368, 379 (1963) (same); United States v. Classic, 313 U.S. 299, 314 (1941) (the right to vote for Congressmen, and by extension participate in congressional primaries, is found in Article I, Section II of the constitution).

[58] *Gray*, 372 U.S. at 381.

[59] See Williams v. Rhodes, 393 U.S. 23, 30 (1968) (noting that restrictions are impermissible when they burden "the right of qualified voters . . . to cast their votes effectively"); *Reynolds*, 377 U.S. at 555 (noting that "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").

[60] *Bush,* 531 U.S. at 109 ("[T]here must be at least some assurance that the rudimentary requirements of equal treatment and fundamental fairness are satisfied."); see also *Reynolds,* 377 U.S. at 555 (citations omitted) ("The right to vote can neither be denied outright, nor destroyed by alteration of ballots, nor diluted by ballot-box stuffing"); *Gray*, 372 U.S. at 380 ("Every voter's vote is entitled to be counted once. It must be correctly counted and reported."); *South v. Peters,* 339 U.S. 276, 279 (1950) (Douglas, J., dissenting) ("The right to

voting systems, a number of technology-related challenges ensued, because of what *Bush* said and did not say and what states did and did not do.

The first round of voting technology challenges sought to enforce uniform adoption of electronic voting technology under the Equal Protection and Due Process clauses.[61] Studies showed that paper-based punch cards and optically scanned ballots caused a greater number of votes to be invalidated in predominantly African-American precincts than elsewhere—a "racial gap" in the residual vote rate, or probability that votes would be counted inaccurately.[62] States rendered such challenges moot by implementing electronic voting systems statewide, reducing the residual vote rate by one million between 2000 and 2004.[63]

Challenges also arose in states whose counties purchased different *types* of technology. For example, in *Weber v. Shelley*, the plaintiffs argued that although voting equipment reduced under- and over-votes in the aggregate, it still did not distribute the residual vote rate equally across all groups and thus violated the Equal Protection and Due Process clauses.[64] Because machines have varying levels of accuracy, by using one machine in some counties but not everywhere, the state subjected voters to different probabilities that their votes would be counted accurately. The challenge failed. The court found that the electronic system in use did not restrict the right to vote *severely enough* to justify relief.[65] Courts facing these sorts of challenges cite Justice Souter's dissent in *Bush*, which justified the use of different technologies across

---

vote includes the right to have the ballot counted."); United States v. Saylor, 322 U.S. 385, 387–88 (1944) (noting that the right to vote includes the right to have vote counted); *Classic*, 313 U.S. at 315 ("Obviously included within the right to choose . . . is the right of qualified voters . . . to cast their ballots and have them counted.").

[61] See, e.g. Stewart v. Blackwell, 444 F.3d 843, 852 (6th Cir. 2006), superseded as moot by Stewart v. Blackwell, 473 F.3d 692 (6th Cir. 2007). The Court noted that "[v]iolations of the Equal Protection Clause are no less deserving of protection because they are accomplished with a modern machine than with outdated prejudices." Id. at 880.

[62] Michael Tomz & Robert P. Van Houweling, How Does Voting Equipment Affect the Racial Gap in Voided Ballots?, 47 Am. J. of Pol. Sci. 46, 58 (2003); see also Daniel P. Tokaji, The Paperless Chase: Electronic Voting and Democratic Values, 73 Fordham L. Rev. 1711, 1754–68 (2005) (arguing that electronic technology can reduce or eliminate the racial disparities resulting from punch-card systems).

[63] Charles Stewart III, Residual Vote in the 2004 Election, 5 Election L.J. 158, 158 (2006).

[64] 347 F.3d 1101, 1101, 1106 (9th Cir. 2003).

[65] *Weber*, 347 F.3d at 1106; see also Wexler v. Anderson, 452 F.3d 1226, 1233 (11th Cir. 2006) (holding that different voting methods have different trade-offs, and the state's important regulatory interests justify choosing between them).

election jurisdictions based on "concerns about cost, the potential value of innovation, and so on."[66]

Beyond the challenges presented by the holding in *Bush*, voting-technology challenges continued to fail because of the standard of scrutiny established by *Anderson v. Celebreze*[67] and *Burdick v. Takushi*[68] (referred to as the *Anderson–Burdick* sliding scale test). Under the *Anderson-Burdick* sliding scale test, courts apply strict scrutiny to an election administration practice, such as what voting technology to buy or maintain, only if it is unreasonable and discriminatory or if it imposes a "severe" burden on voters.[69] If the burden is "reasonable" and "nondiscriminatory," or it is not severe, then it is constitutional if the state demonstrates an "important regulatory interest[]"[70] or even "legitimate and valid" concerns.[71] *Anderson-Burdick* is the workhorse of election administration law, even though it is arguably in deep tension with the central holding of *Harper v. Virginia Board of Elections*, which is that any practice that burdens the right to vote and that is unrelated to voter qualifications, not just outright proscriptions of the franchise, should receive strict scrutiny.[72] Indeed, *Harper* said that "[t]he degree of the discrimination is irrelevant"[73] precisely because the voter regulation at issue there (a poll tax in order to obtain a ballot) was unrelated to voter qualifications. Presumably, then, something far less severe than a poll tax

---

[66] See, e.g., *Wexler*, 452 F.3d at 1233 (citing Bush v. Gore, 531 U.S. 98, 134 (2000) (Souter, J., dissenting));*Weber*, 347 F.3d at 1107 & n. 2 (citing the same).

[67] 460 U.S. 780, 788 (1983).

[68] 504 U.S. 428, 434 (1992).

[69] *Burdick*, 504 U.S. at 434 (citations omitted) ("[T]he rigorousness of our inquiry into the propriety of a state election law depends upon the extent to which a challenged regulation burdens First and Fourteenth Amendment rights. Thus, as we have recognized when those rights are subjected to 'severe' restrictions, the regulation must be 'narrowly drawn' to advance a state interest of compelling importance. But when a state election law provision imposes only 'reasonable, nondiscriminatory restrictions' upon the First and Fourteenth Amendment rights of voters, 'the State's important regulatory interests are generally sufficient to justify' the restrictions.").

[70] *Burdick*, 504 U.S. at 434; *Anderson*, 460 U.S. at 788; Storer v. Brown, 415 U.S. 724, 730 (1974) (noting that "as a practical matter, there must be a substantial regulation of elections if they are to be fair and honest and if some sort of order, rather than chaos, is to accompany the democratic processes").

[71] Rosario v. Rockefeller, 410 U.S. 752, 761–62 (1973).

[72] 383 U.S. 663, 670 (1966) ("We have long been mindful that where fundamental rights and liberties are asserted under the Equal Protection Clause, classifications which might invade or restrain them must be closely scrutinized and carefully confined . . . . Those principles apply here.").

[73] *Harper*, 383 U.S. at 668.

as a condition for obtaining a ballot would trigger strict scrutiny if it were unrelated to voter qualifications. Yet, under *Anderson-Burdick*, the degree of a burden, even one that has nothing to do with voter qualifications such as voting technology that counts votes with varying degrees of accuracy, seems to be a *threshold* question as well as a dispositive one.

The Court applies *Anderson-Burdick* to election administration because of the basic difficulties of administering elections.[74] Voters cannot expect perfection across jurisdictions because it is impracticable to ever fully equalize burdens. Some voters will always live farther from polling places. It will always be harder for some voters to obtain photo identification. Lines will always be longer and ballots more confusing for some voters. Some jurisdictions will always have fewer dollars or political capital to update voting equipment and will thus use older machines with greater residual vote rates. That is the inescapable reality of election administration, or so it seems. To require otherwise, in the Court's view, would hamstring local officials seeking to impose order on a chaotic democratic process.[75] Thus, at least in the context of voter technology, states can treat dissimilar people who are similarly situated differently without running afoul of the Equal Protection Clause.

Essentially, then, *Bush* and its progeny suggest that unequal residual vote rates are symptomatic of inevitably imperfect technologies. *Bush* and its progeny also suggest those rates are innocuous, in that they are beyond the reach of the constitution's right to vote, because they are reasonable, nondiscriminatory, and do not *severely* burden that right. Election hacking, however, has forced at least one court to revisit that calculus.

III. HACKING THE RIGHT TO VOTE

Hacking sits squarely at the intersection of the Court's right-to-vote jurisprudence and issues surrounding voting technology. For example, in

[74] *Burdick*, 504 U.S. at 433 ("Election laws will invariably impose some burden upon individual voters."); *Anderson*, 460 U.S. at 788 ("Each provision [of election administration], whether it governs the registration and qualifications of voters, the selection and eligibility of candidates, or the voting process itself, inevitably affects—at least to some degree—the individual's right to vote.").

[75] *Storer*, 415 U.S. at 730 ("[A]s a practical matter, there must be a substantial regulation of elections if they are to be fair and honest and if some sort of order, rather than chaos, is to accompany the democratic process."); see also *Burdick*, 504 U.S. at 433 (explaining that subjecting every voting regulation to strict scrutiny would "tie the hands of States seeking to assure that elections are operated equitably and efficiently").

Curling v. Kemp, the United States District Court for the Northern District of Georgia found that challengers to Georgia's statewide voting technology provided sufficient evidence to show, on the basis of a factual record that was yet to be fully developed, "that their votes cast by DREs may be altered, diluted, or effectively not counted."[76]

First, the court did not discuss whether a particular residual vote rate must be found in order to find a right-to-vote violation.[77] In fact, because it was a pre-election challenge, no such finding was *possible*.

Second, the challengers actuall*y* showed "serious security flaws and vulnerabilities," as opposed to pointing to merely theoretical or hypothetical flaws, including "outdated software susceptible to malware and viruses."[78] This showing established "a concrete," nonspeculative risk that ballots could be altered in a way that undermines the opportunity to cast an effective vote.[79]

Finally, the court dismissed Georgia's argument, at the motion-to-dismiss stage, that the injury to challengers' right to vote was caused by hackers rather than the state.[80] States typically have no duty to protect citizens from privately inflicted harms, but the court found that, for at least the purposes of the motion to dismiss stage, there was a plausible

[76] Curling v. Kemp, 334 F. Supp. 3d 1303, 1324–25 (N.D. Ga. 2018) (noting the court's conclusion that the plaintiffs were likely to succeed on the merits of one or more of their constitutional claims, in the context of a motion for a preliminary injunction, was a "cautious, preliminary one, especially in light of the initial state of the record," but that the evidence sufficiently showed that "votes cast by DRE may be altered, diluted, or effectively not counted on the same terms as someone using another voting method – or that there is a serious risk of this under the circumstances").

[77] While at least one court in the post-*Bush* era expressly declined to specify a precise error rate for determining when voting technology is constitutional and when it is not, see Stewart v. Blackwell, 444 F.3d. 843, 876 (6th Cir. 2006), it applied strict scrutiny based on a fully developed factual record indicating that in ten counties in Ohio the residual vote rate was over 3% in the 2000 election, id. at 872, while intentional undervoting makes up an estimated 0.23% to 0.75% of all residual votes, id. at 848, and that approximately 55,000 votes were lost in the 2000 presidential election statewide. Id. at 871. The *Stewart* court went so far as to say that the disparate technology at issue would fail even rational-basis review. Id. at 872; see also; *Black v. McGuffage*, 209 F.Supp.2d 889, 893, 899 (N.D. Ill. 2002) (finding that plaintiffs sufficiently stated an equal protection claim where jurisdictions without error notification had an average residual vote rate of 3.85%, but jurisdictions with error notification had an average residual vote rate of less than 1%).

[78] *Curling*, 334 F.Supp.3d at 1308, 1322. (featuring testimony of Dr. Alex Halderman, a computer scientist at the University of Michigan, showing "how a malware virus can be introduced into the DRE machine by insertion of an infected memory card (or by other sources) and alter the votes cast without detection").

[79] Id. at 1324.

[80] Id. at 1317.

causal connection, even if only indirectly, between the state's use of unsecure DREs and the injury to challengers' constitutional rights.[81]

The nature of hacking is the chief reason why *Curling* stands apart from *Bush* and its progeny. At the end of an election, there will be no way to determine the accuracy of a vote count. Post-*Bush* courts did not foresee this possibility. In one case, for example, the Eleventh Circuit rejected an equal protection challenge based on differing methods manual recounting to determine whether machines registered the correct number of no-votes, because the mere possibility of an "allegedly inferior type of review" in the event of a manual recount was not so substantial a burden as to warrant strict scrutiny.[82]

Hacking, on the other hand, conceals its own detection. Malicious code that modifies vote counts hides evidence of its existence by also modifying the audit logs, vote records, and protective counters stored by the machine that are installed as countermeasures.[83] Even electronic ballot "images are themselves subject to manipulation by hackers."[84] Given the archaic nature of election machines, a post-election investigation will not find evidence that anything went awry. Courts cannot rely on the absence of evidence of tampering or malfunction as evidence of absence of accuracy issues, or as evidence of user error, in the hacking era.

Hacking is no longer a far-off risk, either, but rather a near certainty. It is easy to manipulate vote tabulations even if voting machines are disconnected from the internet, or "air-gapped." Hackers can access machines through the modems that transmit vote totals on election night.[85] Hackers can "compromise voting equipment at many points along the supply chain, from the factory assembler to the election software programmer to the technician who makes a repair or installs a software upgrade."[86] Hackers could also commandeer remote access software that allows contractors to make updates from home, or infect installable memory cards that are carried to central-counting facilities to upload

[81] Id. at 1317.

[82] Wexler v. Anderson, 452 F.3d 1226, 1232–33 (11th Cir. 2006).

[83] *Curling*, 1303 F.Supp.3d at 1308–9 (Dr. Halderman demonstrated that "[t]he DRE machine's paper tape . . . confirmed the same total number of votes, including the results of the manipulated or altered votes" in spite of the fact that the machines "record individual ballot data in the order in which they are cast and they assign a unique serial number and timestamp to each ballot").

[84] De la Garza, supra note 4.

[85] Zetter, supra note 18.

[86] Wines, supra note 16.

votes.[87] Hackers can even compromise computers in election offices, then spread malicious code to voting machines when election officials program ballots.[88]

Admittedly, it is harder to manipulate vote tabulations in a way that picks winners and losers—but this is because of an information gap, not a technology gap. To effectively do so, hackers "would have to know which districts could affect the outcome. Then they'd have to change just enough votes to ensure victory without switching so many that it would draw attention."[89] All the same, *Curling* suggests that antiquated voting systems are hackable voting systems and hackable voting systems violate the right to vote. This is not to suggest that the right to vote requires something that is not theoretically possible, i.e., unhackable voting machines. It is only to suggest that states must not sit idly by while vulnerabilities create arbitrary disparities in whether votes will be counted accurately.

IV. ACCESS HACKS: THIRD-GENERATION INFRINGEMENTS ON THE RIGHT TO VOTE

Manipulating vote tabulation is not the only way to hack an election. "Access hacks" have the effect of placing obstacles before voters that frustrate their ability to effectively participate in the voting process. The problem is that voting operations seem to be designed to perform the simple task of casting a ballot in an overcomplicated way, like a Rube Goldberg machine. Vulnerabilities include not just machinery, but websites, registration databases, e-pollbooks, and recording and reporting systems—systems that hackers could exploit to aggregate countless low-value burdens on voters. This is the third generation, or perhaps the final frontier, of voting infringements.[90] Although harder to address in court,

[87] Zetter, supra note 18.

[88] Halpern, supra note 41. Dr. J. Alex Halderman, a computer scientist and expert witness in *Curling*, demonstrated this point at Def Con's Voting Village on a machine that remains in use in eighteen states. Id.

[89] Massimo Calabresi, The Secret History of Election 2016, Time (July 31, 2017), [https://perma.cc/L8K2-FPXQ].

[90] See generally Carol Anderson, One Person, No Vote: How Voter Suppression is Destroying Our Democracy (2018) (summarizing modern voter suppression efforts); Desmond Ang, Do 40-Year-Old Facts Still Matter? Long-Run Effects of Federal Oversight Under the Voting Rights Act 2, 39 (Harvard Kennedy Sch. Faculty Research Working Paper Series, Paper No. RWP18-033, 2018), [https://perma.cc/8M6N-UNKT] (finding suggestive early evidence that voting protections have been greatly eroded in the five years since the Court's holding in *Shelby County, Alabama v. Holder*, 570 U.S. 2 (2013), that the Voting

given existing right-to-vote doctrine, these risks can be mitigated with system updates.

Legacy systems contain known vulnerabilities that can disrupt election infrastructure. Hackers can take down voting machines through a Distributed Denial of Service ("DDoS") attack. In North Carolina in 2016, an alleged software glitch demonstrated the chaos that an attack on infrastructure could cause, such as machine crashes, long lines, extended hours, and back-up paper ballots (if counties have them, which is by no means a guarantee).[91] Long lines destroy voter confidence "even when individuals do not experience the long lines themselves" because voters could decide that voting simply is not worth the trouble or wait.[92] Hackers can also crash e-pollbooks, which election officials often use to check-in voters on Election Day. In 2006 in Denver, for example, an e-pollbook malfunction caused about 20,000 people to leave polling places without voting.[93] In 2008 in Georgia, a similar malfunction caused two-hour-plus lines.[94]

Similarly, legacy databases are vulnerable to information exploitation, where hackers manipulate voter records to increase frustration and foil participation. Hackers could access databases to change precinct assignments to send voters to the wrong location, wasting time and costing votes.[95] In 2016, when a Russian agent logged into a single election jurisdiction's database in Illinois, he opened a backdoor to the files on all of the state's voters in all 109 jurisdictions' statewide since 2006.[96] He then gained access to 15 million voter registrations, stole 90,000 files, and attempted, albeit unsuccessfully, to change voter information including names and addresses.[97] Likewise, in California's 2016 presidential primary, hackers used private voter information,

Rights Act's continued coverage based on historical, rather than current, measures of discrimination is unconstitutional).

[91] Perlroth et al., supra note 52.

[92] Charles Stewart III & Stephen Ansolabehere, Waiting in Line to Vote, Executive Summary (CalTech/MIT Voting Project, Working Paper No. 114, 2013), [https://-perma.cc/T7KK-AH9N]; Voting Technology Project, supra note 7, at 32 (explaining that in the 2000 election, approximately one million voters said that they did not vote because the line was too long or the hours were too short).

[93] Zetter, supra note 18.

[94] Id.

[95] See id.

[96] See Calabresi, supra note 89, at 34.

[97] Id. at 34–35.

including Social Security numbers, to change voter registrations in the state's database, preventing a number of voters from casting ballots.[98]

Hackers can even take advantage of state voter restrictions to disrupt elections and sow division. To illustrate this issue, consider Georgia. Just before Election Day in 2018, officials used an exact match voter registration law to stall over 50,000 voter registrations containing information that was inconsistent, they argued, with drivers-license records, such as mismatched signatures, omitted middle initials, misspelled names, and missing hyphens.[99] They rejected a number of absentee ballots for similar reasons.[100] A disproportionate number of voters facing stalled registrations and rejected absentee ballots were black.[101] Georgia's secretary of state, who is now governor, used Georgia's exact-match voter registration law as a justification for the mass suspension.[102] Hackers could exploit Georgia's oppressive law and others like it to precisely the same effect. By altering voter registrations to make them inconsistent with drivers-license records, hackers could depress turnout, suppress or functionally deny the vote, or change the outcome of the election. To be sure, thirty-one states introduced ninety-nine bills impeding access to registration and voting in 2017,[103] so the target market is a mile wide and the firewalls an inch deep.

V. CONCLUSION

It is difficult to square the extent to which we value the right to vote with the state of voting technology. Federalism, funding, and industry get in the way. Courts must then act as the forum of last resort. However, in the wake of *Bush*, technology became a solution in search of a problem, enabling the hacks that now imperil the right to vote. *Bush*'s progeny provided little recourse until *Curling*, where the unique nature, unparalleled scope, and concrete threat of hacking brought the vulnerability of voting machines into sharp relief. *Curling* offers promise in an area of the law where there is mostly peril. Moreover, although right-to-vote jurisprudence, even *Curling*, has little to say about what happens

[98] Id. at 32.

[99] See Astead W. Herndon, Georgia Voting Begins Amid Accusations of Voter Suppression, N.Y. Times (Oct. 19, 2018), [https://perma.cc/A9N7-RHA7].

[100] Id.

[101] Id.

[102] Id.

[103] Voting Laws Roundup 2017, Brennan Ctr. for Just. (May 10, 2017), [https://perma.cc/G6UF-SKVX].

when hackers target information databases in order to increase frustration and thwart participation, sensible system upgrades and security protocols may reduce the likelihood of such threats. In short, judges have a role to play in holding states accountable, states must play a role in providing support to local officials across 10,000 election jurisdictions, and voters must begin demanding changes through their exercise of the franchise—by resort to the very polls that are endangered by hackers—and in keeping the faith otherwise.