Counting the Votes: Electronic Voting Irregularities, Election Integrity, and Public Corruption

KIMBERLY BREEDON* & A. CHRISTOPHER BRYANT**

"I consider it completely unimportant who . . . will vote, or how; but what is extraordinarily important is this—who will count the votes, and how."

Joseph Stalin (apocryphal)

* Visiting Professor, University of Cincinnati College of Law.

** Rufus King Professor of Constitutional Law, University of Cincinnati College of Law. The authors thank all the participants in the March 15, 2019, University of Memphis Law Review Symposium for their comments and suggestions. Thanks also to the University of Cincinnati and the Harold C. Schott Foundation for financial support. Of course, remaining errors are ours alone.

I. INTRODUCTION

Most treatments of barriers to the ballot box—understandably and appropriately—focus on commonly recognized obstacles to casting votes, including: voter ID requirements; voter-roll purges; limitations on early voting and absentee voting; felon disenfranchisement; voter registration impediments; gerrymandering; and disinformation about voting procedures, requirements, and locations. Less commonly treated are voting irregularities that occur after voting has ended. These irregularities include flipped votes, added votes, uncounted votes, and purged votes. Typically, these irregularities occur in voting precincts that employ electronic voting machines.

Even more rarely discussed is the role that election officials' conflicts of interest may play in impeding efforts to ensure that the electronic voting machines are in good working order and are free from vulnerabilities to hacking or malware.[1] A few states use electronic voting machines to tally votes, without providing for any kind of accompanying paper trail. In the event of Election Day irregularities, the electronic audit processes are often entirely unavailable or under the control of government officials with demonstrated conflicts of interest who may decline to pursue an audit. In the absence of an uncorrupted audit, any voting tallies that have been subject to tampering will go undetected; but the irregularities giving rise to the need for an audit may nevertheless cast suspicion over the integrity of the outcome.[2]

We argue that, in this era of growing distrust in our nation's voting systems, the conception of voting barriers should be expanded to include potential conflicts of interest held by public officials who are entrusted with ensuring the integrity of the systems and procedures adopted for accurate vote counting. More broadly, we build upon our

---

1. For a notable exception, albeit outside the formal legal literature, see Sue Halpern, *How Voting-Machine Lobbyists Undermine the Democratic Process*, NEW YORKER (Jan. 22, 2019), https://www.newyorker.com/tech/annals-of-technology/how-voting-machine-lobbyists-undermine-the-democratic-process (documenting the relationship of election officials and voting machine lobbyists in Georgia and Delaware).

2. *See* Stephanie Phillips, Comment, *The Risks of Computerized Election Fraud: When Will Congress Rectify a 38-Year Old Problem?*, 57 ALA. L. REV. 1123, 1141–42 (2006) (internal citations omitted) (discussing issues with Direct Record Electronic Voting Systems and how the lack of audit trails could sow a public perception of dishonesty).

prior work on public corruption[3] to argue that the role that electronic voting irregularities play in undermining faith in our elections' integrity has received insufficient attention from lawmakers, and we explore possible mechanisms for addressing the problem.

Our argument proceeds as follows: Part II briefly reviews the theoretical and constitutional implications of vote-count integrity, stressing the importance of public confidence as a crucial concern even in the absence of actual fraud or falsification. Part III provides a basic survey of current practices and vulnerabilities in states that use electronic voting machines but do not have paper ballots as back-up records for voting tallies and post-election audits. Part IV examines the potential conflicts of interest that may influence a public official's decision about the purchase of electronic voting machines or operating software, as well as whether, or how aggressively, to pursue an audit in an election for which some evidence exists that the outcome was tainted. We also suggest a rubric grounded in private trust for evaluating and avoiding such conflicts. Finally, Part V critiques current legislative proposals proffered as steps to address the vulnerabilities of the voting procedures in place in many major American jurisdictions, and Part VI briefly concludes.

II. DEMOCRACY, DOUBTS, AND DANGERS

Few, we hope, would question the importance of accuracy in vote tallying. It is, after all, indispensable to the realization of the central promise of popular government; namely, that the largest portion of the electorate will control the selection of representatives. Nevertheless, some components of the importance of reliability in vote counting may be less obvious, as perhaps are the constitutional dimensions of the issue. Accordingly, we pause to recite them briefly.

More likely to be underappreciated, and yet still central to our claims in this Essay, is the gravity of the danger of *any* public suspicion, whether well-founded or not, on the trustworthiness of the vote tallies.

---

3. *See* Kimberly Breedon & A. Christopher Bryant, *The Brand v. The Man: Considering a Constructive Trust as a Remedy for President Trump's Alleged Violations of the Foreign Emoluments Clause*, 9 CONLAWNOW 111 (2018); Kimberly Breedon & A. Christopher Bryant, *The Potential Roles of the Constructive Trust and the Blind Trust as Remedies for Emoluments Clause Violations*, 11 ALB. GOV. L. REV. 284 (2018).

The seriousness of the harms threatened by such suspicions is demonstrated by the fact that hostile foreign powers have expended substantial resources in an effort to sow these suspicions' seeds.[4] As we explain below, these forces, averse to the very project of democratic self-government, have recognized that public doubts about the integrity of vote counting crack the foundation on which the edifice of elections rests.

* * *

The premise of electing representatives is that their selection should be made by the largest percentage of the electorate to unite in support of a candidate. Anything else would subvert the ideal of republican self-government. Less obvious, perhaps, but still fundamental to our governing order is the role that elections play as a check on the abuse of governmental power. As Professor Zephyr Teachout observed in her seminal article, *The Anti-Corruption Principle*,[5] when the Framers debated and fashioned the Constitution's electoral provisions, an overarching concern was ensuring the electorate's ability to jettison corrupt officials.[6] And more than two centuries later it remains the case that "[v]oting politicians out of office is, in many cases, the only direct remedy for the public" to obtain redress for abuses of trust by government officials.[7] Not surprisingly, when representatives do succumb to corrupting influences, they in turn frequently seek to disrupt the mechanisms in place for holding them accountable. As a report recently published by Transparency International noted, "when corruption seeps

4. LAWRENCE NORDEN & IAN VANDEWALKER, BRENNAN CTR. FOR JUST., SECURING ELECTIONS FROM FOREIGN INTERFERENCE 3–4 (2017), https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_1.pdf (documenting the various federal agency reports of foreign interference in the 2016 federal election).

5. Zephyr Teachout, *The Anti-Corruption Principle*, 94 CORNELL L. REV. 341, 397–408 (2009) (arguing that, like the "separation-of-powers principle," the Constitution entrenches an implied "anti-corruption principle" that should serve as a hermeneutic tool in constitutional interpretation and analysis).

6. *Id.* at 362 ("Regular legislative elections were intended as one of the most important checks on corruption."); *see also id.* at 362–64 (describing the deliberations surrounding the frequency of legislative elections for the House and Senate).

7. Claire Hill & Richard Painter, *Compromised Fiduciaries: Conflicts of Interest in Government and Business*, 95 MINN. L. REV. 1637, 1645 (2011).

into the democratic system, corrupt leaders may seek to prevent democratic checks and balances so that they can continue to remain in power unpunished."[8] Obviously to the extent that vote tallies are vulnerable to manipulation, elections may fail to serve their function of checking governmental abuse.

The Supreme Court has repeatedly reiterated that the Constitution treats the right to vote as fundamental.[9] In *Reynolds v. Sims*, the landmark case recognizing the core "one person, one vote" principle, the Court remarked:

> Undeniably the Constitution of the United States protects the right of all qualified citizens to vote, in state as well as in federal elections. . . . The right to vote freely for the candidate of one's choice is of the essence of a democratic society, and any restrictions on that right strike at the heart of representative government.[10]

That same year the Court elaborated that "[n]o right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live," and that all "[o]ther rights, even the most basic, are illusory if the right to vote is undermined."[11] More recently, and succinctly, the Court declared simply that "[i]t is beyond cavil that 'voting is of the most fundamental significance under our constitutional structure.'"[12] Of course, this right extends beyond the mere casting of a ballot to a right that a ballot properly cast be accorded full and equal significance. More than a century ago, the Justices explained, "[w]e regard it as equally unquestionable that the right to have one's vote counted is as open to protection

8. Coralie Pring & Jon Vrushi, *Tackling the Crisis of Democracy, Promoting Rule of Law and Fighting Corruption*, TRANSPARENCY INT'L (Jan. 29, 2019), https://www.transparency.org/news/feature/tackling_crisis_of_democracy_promoting_rule_of_law_and_fighting_corruption.

9. *See, e.g.*, Burdick v. Takushi, 504 U.S. 428, 433 (1992); Wesberry v. Sanders, 376 U.S. 1, 17 (1964); Reynolds v. Sims, 377 U.S. 533, 555 (1964).

10. *Reynolds*, 377 U.S. at 554–55.

11. *Wesberry*, 376 U.S. at 17.

12. *Burdick*, 504 U.S. at 433 (quoting Illinois Bd. of Elections v. Socialist Workers Party, 440 U.S. 173, 184 (1979)).

. . . as the right to [cast a vote]";[13] the Court echoed this sentiment decades later in the observation that "[o]bviously included within the right to choose [representatives], secured by the Constitution, is the right of qualified voters within a state to cast their ballots *and have them counted*."[14]

Though necessary, it is far from sufficient that all votes be counted. It is as imperative that the public *believe* that the vote tallies are accurate. Indeed, public doubts about vote-count integrity may ultimately prove as destructive to democratic processes as actual tampering. Elections succeed in their purpose of resolving differences and conferring legitimacy only to the extent that they enjoy public confidence.[15] A people *may* temporarily acquiesce in an election result perceived as tainted, but even so, the long-term impact of the perception will be wide-spread disaffection with the political process, disengagement from public discourse and political campaigns, and alienation from both the government and the laws it seeks to uphold.[16] No gov-

13. United States v. Mosley, 238 U.S. 383, 386 (1915).

14. United States v. Classic, 313 U.S. 299, 315 (1941) (emphasis added); *see also Reynolds*, 377 U.S. at 555 (first citing *Ex parte Yarbrough* ("The Ku-Klux Cases"), 110 U.S. 651 (1884); and then citing United States v. Mosley, 238 U.S. 383 (1915)) ("It has been repeatedly recognized that all qualified voters have a constitutionally protected right to vote *and to have their votes counted*.") (emphasis added).

15. *See, e.g.*, Curling v. Kemp, 334 F. Supp. 3d 1303, 1324 (N.D. Ga. 2018) ("Ultimately, an electoral system must be accurate *and trustworthy*.") (emphasis added). As plaintiffs in *Fair Fight Action v. Crittenden* stated in their Complaint, "[f]air elections ensure the consent of the governed; they are the moral foundation of the compact between the government and its citizens." Complaint at 1, Fair Fight Action v. Crittenden, No. 1:18-cv-05391-SCJ, 2018 WL 6187610 (N.D. Ga. Nov. 27, 2018); *see also* Halpern, *supra* note 1 ("The practice of democracy begins with casting votes; its integrity depends upon the inclusivity of the franchise and the accurate recording of its will.").

16. Daniel Stockmeyer et al., *Bribes and Ballots: The Impact of Corruption on Voter Turnout in Democracies*, 34 INT'L. POL. SCI. REV. 74, 82 (2011) ("Corruption . . . undermines good governance, the rule of law, economic development, and moral values [and] also hinders citizens' participation in elections."); Kim Zetter, *The Crisis of Election Security*, N.Y. TIMES MAG. (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html:

> The ballot box is the foundation of any democracy. It's not too grand to say that if there's a failure in the ballot box, then democracy fails. If the people don't have confidence in the outcome of

ernment has the capacity to compel obedience by force alone; free societies therefore depend on voluntary compliance with the laws, even (perhaps especially) by those who may believe particular laws to be unwise or unjust. In the absence of credible elections, societies face a stark choice between, on the one hand, a brutal authoritarianism resting on the sum of force and fear and, on the other hand, anarchy.

In the hopes of demonstrating that no third, stable alternative exists, authoritarian foreign regimes have systematically sought to undermine public confidence in elections—targeting Western democracies in general and, at least since the 2016 general election, the U.S. specifically.[17] Cybersecurity experts classify those seeking to interfere with electoral processes into two general categories of malign actors: In the first category are actors "who seek to actively manipulate the election so that their preferred candidate is illegitimately declared the winner."[18] In the second category are actors "that seek to undermine confidence in the vote, so that a defeated candidate can protest the outcome in a way that prompts at least some doubt in the general populace."[19] The actors in this category have at their disposal multiple mechanisms for achieving their goal of casting doubt on the legitimacy

---

> an election, then it becomes difficult for them to accept the policies and actions that pour forth from it.

17. Michael Chertoff & Anders Fogh Rasmussen, *The Unhackable Election: What It Takes to Defend Democracy*, FOREIGN AFFAIRS (Jan./Feb. 2019), https://www.foreignaffairs.com/articles/2018-12-11/unhackable-election. In a Grand Jury indictment handed down on July 13, 2018, the United States charged twelve Russian military intelligence operatives for, among other conduct, hacking into the election systems of multiple states and local voting precincts. Indictment, United States v. Netyksho, No. 1:18-cr-00215-ABJ (D.D.C. July 13, 2018); *see also* Robert McMillan & Dustin Volz, *Voting Machine Used in Half of U.S. Is Vulnerable to Attack, Report Finds*, WALL ST. J. (Sept. 27, 2018, 8:40 AM), https://www.wsj.com/articles/widely-used-election-systems-are-vulnerable-to-attack-report-finds-1538020802 ("Russian hackers were accused by U.S. intelligence agencies of probing the election infrastructure of at least 21 states, breaching a small number of voter-registration databases, and promoting divisive propaganda on social media.").

18. Ben Buchanan & Michael Sulmeyer, *Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity*, BELFER CTR. FOR SCI. & INT'L AFFAIRS 12 (Oct. 2016), https://www.belfercenter.org/sites/default/files/files/publication/hacking-chads.pdf.

19. *Id.*

of an election.[20] The very fact that these hostile foreign regimes have dedicated enormous resources over extended periods[21] to create doubts about electoral integrity provides powerful testimony to such doubts' destructive potential.

When election irregularities arise, including through evidence of hacking attempts or claims of manipulation, candidates can contribute, often unwittingly, to perceptions of illegitimacy by refusing to concede a closely contested election or by alleging impropriety.[22] Concession of an electoral race by a losing candidate and the peaceful transfer of power are pillars of a healthy democracy. The mere possibility that hacking may have occurred can undermine both pillars; and a losing candidate who relies on "irregularities as signs of broader foul play" to resist conceding or allege impropriety may do lasting damage to democratic processes and institutions.[23]

Importantly, cries of foul play by a candidate who ultimately wins can also engender perceptions of illegitimacy. The 2018 midterm elections were witness to close races for several elected offices, including the governor's race in Georgia and the United States Senate race in Florida. In both races, the winning candidate falsely accused his opponents of criminal conduct relating to the election, including an unfounded allegation of computer hacking in Florida.[24]

---

20. According to Buchanan and Sulmeyer, hackers who cause even just a few discernible irregularities can engender "a perception of illegitimacy" of the election as a whole. *Id.* at 14. This is so because evidence of a hacking attempt, regardless of whether such attempt was successful, potentially creates a misperception that hackers succeeded in their efforts elsewhere. For example, hackers may deliberately provide evidence of their efforts by posting videos showing their manipulation of electronic votes or other unauthorized access to voting systems. "These kinds of communications—part-boast, part-threat, part-influence operation—have gained such prominence as to become their own genre . . . ." *Id.* at 14–15.

21. *See* Indictment, United States v. Netyksho, No. 1:18-cr-00215-ABJ (D. D.C. July 13, 2018).

22. Buchanan & Sulmeyer, *supra* note 18, at 15.

23. *Id.*

24. *See* Lawrence Mower & Samantha J. Gross, *FDLE Silent as Rick Scott and Pam Bondi Seek Voter Fraud Investigation*, TAMPA BAY TIMES (Nov. 12, 2018), https://www.tampabay.com/florida-politics/buzz/2018/11/12/fdle-silent-as-rick-scott-and-pam-bondi-seek-voter-fraud-investigation ("Gov. Rick Scott has repeatedly gone on TV to complain of 'rampant fraud' in Tuesday's election after witnessing his lead in the U.S. Senate race against Democratic Sen. Bill Nelson dwindle as votes continued to be counted after election night. . . . [H]e's offered no evidence of fraud

Regardless of which type of malign actor is involved in an effort to interfere with the integrity (or perception of integrity) of a given election, the candidate who benefits from the manipulation does not even need to be aware of the efforts made on his or her behalf to exacerbate the problem of perceived illegitimacy.[25] To contest a tight election, such candidates need only have the capacity to convince themselves that they won the election or to believe that their political opponents are capable of engaging in dirty tricks.[26]

A losing candidate presented with evidence that hacking or claims of manipulation tainted vote tallies "may seize on any irregularities as signs of broader foul play," regardless of whether the hackers' action failed to flip the election to their preferred candidate.[27] But changing the outcome is not necessary to jeopardize the perceived legitimacy of an election.[28] In this situation, a malign actor can achieve the goal of election disruption merely by casting doubt on the integrity of the electoral process.[29]

The danger posed by public doubts about vote tallies' integrity compels the conclusion that all reasonable efforts to secure that integrity against suspicion be undertaken. Anything less invites not only tampering but highly destructive fearmongering by those unhappy with an election's outcome. More specifically, those seeking to undermine a particular election or to destabilize American democracy in general are significantly enabled by electoral processes that lack transparency and are vulnerable to tampering not traceable by available audits. Unfortunately, as we explain in Part III, several major American jurisdictions recently decided to adopt or continue the use of electronic voting technologies that precisely present these problems.

---

in his call for an investigation."); Eliza Newlin Carney, *It's Time to Fix American Elections—Again*, AM. PROSPECT (Nov. 15, 2018), https://prospect.org/article/it's-time-fix-american-elections-again.

25. *See* Buchanan & Sulmeyer, *supra* note 18, at 12 (detailing the risks that cybersecurity vulnerabilities in U.S. election systems pose for election integrity).

26. *Id.* at 14–15.

27. *Id.* at 15.

28. *Id.*

29. *Id.*

III. TALLIES, TRAVAILS, AND TRIBULATIONS

To provide context for our discussion of the role that election officials' conflicts of interest, or the appearance thereof, play in undermining public faith in election integrity, this Part addresses current electronic-voting machine configurations and vulnerabilities, the importance of auditable paper trails for ensuring accurate vote counting, and the availability and feasibility of robust auditing mechanisms.

Electronic voting machines can be classified into one of two categories: optical-scan machines or direct-recording electronic machines.[30] Optical-scan machines allow voters to record their votes manually on a paper ballot, which is then scanned, stored as a digital image, and saved to a removable memory card.[31] Direct-recording electronic machines (commonly known as "DREs") allow voters to record their votes digitally on touch screens or similar input devices, which then store the digital ballot electronically.[32] Crucially, the paper trail used in conjunction with optical-scan machines furnishes an auditable record for verifying digital vote tallies.[33] Unfortunately, not all states that use these devices require audits; and even those states that do perform audits often simply re-scan the paper ballots.[34] The DREs used by some states also provide a paper trail (of sorts) by displaying—behind a window on the machine—a printed record of a voter's electronic selection of candidates. The voter can then review the printed record to verify the accuracy of the digital record.[35] Election-security experts contend, however, that these DREs "provide, at best, an obsolescent stopgap [because] most voters never check [the voter-verifiable paper trail to ensure their votes were correctly recorded], and often they are

30. Zetter, *supra* note 16.

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*; *see also* Matt Vasilogambros, *A Voter's Guide to Election Security*, PEW (Nov. 1, 2018), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/11/01/a-voters-guide-to-election-security (noting that, as of November 2018, twenty-six states do not require a post-election audit using paper records).

35. Zetter, *supra* note 16.

hard to audit."[36] Moreover, the DREs used in several jurisdictions produce no paper trail at all.[37]

Some jurisdictions opt for DREs that produce a paper barcode summary of a voter's electronic selection instead of full paper ballots with auditable functions.[38] With this type of DRE, a voter casts his or her vote on a touch screen. The voting machine then produces a printed card reflecting the voter's electoral selections both as a summary in written English and in the form of a barcode. Upon verifying the accuracy of his or her votes, the voter returns the card to the machine, which reads and records the information encoded within the barcode. Although these machines provide a paper trail, and although a voter can ostensibly verify his or her votes by reading the English-language record on the printout, in reality, voter verification is impossible because the voter cannot decipher the barcoded information, and it is only the barcode that is used to count the votes.[39] Reliance on machines that produce barcode summaries runs counter to best practices advice from election security experts because such technology creates an opportunity for malign actors to flip or otherwise alter votes by manipulating programming codes in advance or by hacking the technology remotely.[40] These vulnerabilities could mean that the barcode does not

36. *Media Release: Election Security Experts Applaud City of Fairfax, VA and Orange County, CA for Leading in New Election Integrity Methods*, VERIFIED VOTING FOUND. (Dec. 7, 2018), https://www.verifiedvoting.org/2018-city-of-fairfax-and-orange-county-rla-reports-released.

37. Zetter, *supra* note 16; *see also* J.B. Wogan, *Votes Miscounted? Your State May Not Be Able to Find Out*, GOVERNMENT (Dec. 2, 2016, 11:00 AM), http://www.governing.com/topics/politics/gov-states-vote-election-audits-recounts.html (noting that, as of December 2016, "[fifteen] states do not require paper records that could be compared against electronic vote tallies"). Cybersecurity engineer Marc Schneider lists paperless electronic voting machines as one of the top vulnerabilities in our voting systems. Marc Schneider, *Protect Public Trust by Auditing Elections: It's Easier than You Might Think*, THE HILL (Nov. 3, 2018, 4:00 PM), https://thehill.com/opinion/campaign/414631-protect-public-trust-by-auditing-elections-its-easier-than-you-might-think. The use of wireless devices to transmit vote tallies and internet voting are the other two vulnerabilities he identifies.

38. Halpern, *supra* note 1 (noting that counties in Ohio, Kansas, New Jersey, and Arkansas use this type of electronic voting machine).

39. *Id.*

40. *Id.* (quoting Duncan Buell, University of South Carolina Professor of Computer Science) ("Any time you introduce computer technology, you introduce the probability that, if there is value, somebody is going to try to hack it. . . . If you're

accurately reflect the voter's choice, even though the written summary does, which poses a problem for states that do not require manual post-election audits. Even if the barcode does accurately reflect the voter's choice, the voting machine's electronic "reading" of the barcode could be manipulated in some way that an audit would not catch.

The availability of an auditable paper trail is indispensable for ensuring both accurate vote tallies and public confidence in the same.[41] "Security experts have warned Congress that without paper trails, states are vulnerable to invisible election tampering because votes cannot be reliably audited."[42] In the absence of an auditable paper trail, various methods of electronic vote tampering, including the surreptitious introduction of software coded to flip votes or scramble tabulation systems, might leave no detectable evidence, let alone be correctable by even the most rigorous of audits.[43] These risks are especially acute for states using outdated voting machines, which are more susceptible to hacks.[44]

---

tallying [votes] based on barcodes, you could conceivably have software that [flips] the voter's choices.") (second alteration in original); Ashley Bridges, *Cybersecurity Experts Critical of Proposed Voting System*, WJBF NEWS (Dec. 11, 2018, 6:36 PM), https://www.wjbf.com/news/your-local-election-hq/cybersecurity-experts-critical-of-proposed-electronic-voting-system/1653888009.

41. Wogan, *supra* note 37 ("[A]s it's become clear that without a paper record there's no way to verify vote tallies, computer scientists and election activists have begun pushing for states to not only keep a paper record but to also institute routine post-election audits."). Currently, however, fourteen states use electronic voting machines that have no paper back-up. Schneider, *supra* note 37.

42. Eric Geller, *Colorado to Require Advanced Post-Election Audits*, POLITICO (July 17, 2017, 1:01 PM), https://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631.

43. Frank Bajak, *US Election Integrity Depends on Security-Challenged Firms*, ASSOCIATED PRESS (Oct. 29, 2018), https://www.ap-news.com/f6876669cb6b4e4c9850844f8e015b4c.

44. Edgardo Cortes & Lawrence Norden, *Paper Trails for All: Thanks to Russia, Voting Machines May Be More Secure Than Ever in 2020*, BRENNAN CTR. FOR JUST. (Nov. 13, 2018), https://www.brennancenter.org/print/20877 (noting that "the very oldest of our antiquated systems" are nearly universally deemed by experts to be "among the least secure in the country"); Vasilogambros, *supra* note 34 ("'Voting machines, and especially older models, are susceptible to hacks, even if they're not connected to the internet,' said Lawrence Norden, the deputy director of the Brennan Center's democracy program. 'Even memory cards in central locations in a polling place can be compromised by hackers,' he said.").

But such risks are deeply problematic even for states using newer machines and exist regardless of whether the machines (old or new) are connected to the Internet.[45]

As the potential for tainted elections both grows and becomes more widely known, cybersecurity experts and voting integrity advocates have redoubled their warnings. "Computer Scientists have warned that computerized voting and counting systems are vulnerable to error or malicious subversion, and must be checked using methods that do not rely on the correctness of hardware or software."[46] The unanimous consensus among these experts is that the gold standard for ensuring both the integrity of elections and the public trust in election integrity is the use of paper ballots, including those recorded by optical-scan machines, and manual post-election audits based on the paper ballots.[47] In a letter to the United States Election Assistance Commission, dated October 2, 2018, for example, a coalition of election integrity organizations and security experts wrote: "We recognize the only way to ensure resilience in voting systems is by requiring voter-verified pa-

45. Vasilogambros, *supra* note 34. For detailed accounts of the myriad ways voting machines can be hacked remotely, see Zetter, *supra* note 16, and Jennifer Cohn, *Voting Machines: What Could Possibly Go Wrong?*, N.Y. REV. BOOKS (Nov. 5, 2018, 6:00 AM), https://www.nybooks.com/daily/2018/11/05/voting-machines-what-could-possibly-go-wrong; *see also* McMillan & Volz, *supra* note 17 (describing the means by which hackers can gain remote access to a particular type of voting machine widely used throughout the U.S. and can use that access to change votes).

46. MARK LINDEMAN, VERIFIED VOTING FOUND., CITY OF FAIRFAX, VA: PILOT RISK-LIMITING AUDIT 4 (2018) (citing NAT'L ACADS. OF SCI., ENG'G, & MED., SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY (2018)), https://www.verifiedvoting.org/wp-content/uploads/2018/12/2018-RLA-Report-City-of-Fairfax-VA.pdf; *see also* Halpern, *supra* note 1 (quoting Duncan Buell, University of South Carolina Professor of Computer Science) ("Any time you introduce computer technology, you introduce the probability that, if there is value, somebody is going to try to hack it.").

47. Christopher DeLuzio, *Pennsylvania Commission Issues Urgent Call to Replace Vulnerable Voting Machines*, BRENNAN CTR. FOR JUST. (Sept. 27, 2018) (quoting Brennan Center Counsel Liz Howard's testimony before a Pennsylvania legislative committee) (noting that the "'unanimous national security and scientific community consensus is that replacing all paperless voting machines with equipment that creates a paper record of every vote cast is the simple solution' to bolster the security of elections").

per ballots and robust, manual post-election audits of the paper ballots."[48] These experts based this conclusion in part on the ability of malign actors to tamper with voting outcomes without leaving any trace.[49]

It is worth pausing to emphasize the somewhat counter-intuitive aspects of these observations. We live in a world increasingly characterized by the substitution of electronic record-keeping for paper files—in contexts ranging from banking to academia to medical records—a practice driven by the assumption, likely sound in other settings, that electronic storage of information is not only more convenient and subsequently accessible but also more secure. But in the context of voting, experts' universal assessment is that otherwise non-traceable tampering poses a risk that requires, under present circumstances, the preservation of paper records, at least as a backup available for auditors' review.[50] It may well be that some of the laxity by key actors in this area, which we describe below, can be explained as the product of a false sense of security in the voting context traceable to the ubiquity of electronic records in other areas of contemporary life. If so, that

48. In his Politico article, journalist Eric Geller provides a hyperlink to the letter. *See* Eric Geller, *States Should Ditch Cell Modems in Voting Systems, Election Experts Tell Feds*, POLITICOPRO (Oct. 2, 2018, 4:32 PM) https://subscriber.politicopro.com/cybersecurity/whiteboard/2018/10/states-should-ditch-cell-modems-in-voting-systems-election-experts-tell-feds-2018146; *see also* Cohn, *supra* note 45 ("The only way to know if foreign or domestic actors have altered electronic tallies is to conduct . . . 'evidence-based elections.' This would involve a robust manual audit or manual recount of paper ballots (or other paper record that the voter has reviewed for accuracy), and a secure chain of custody between the election night count and any audit or recount."); Wogan, *supra* note 37.

49. Greg Gordon, *Cyber Experts Cite Vulnerabilities in Washington, North Carolina Voting Security*, MCCLATCHY WASH. BUREAU (Nov. 12, 2018, 8:09 AM), https://www.mcclatchydc.com/latest-news/article221423980.html ("There may be no obvious clue to alert election officials when someone preys on the electronic systems, the [cyber] experts said."); Bajak, *supra* note 43 ("Experts say they have long skimped on security in favor of convenience, making it more difficult to detect intrusions such as occurred in Russia's 2016 election meddling."); Zetter, *supra* note 16 (quoting Matt Blaze, University of Pennsylvania Professor of Computer Science and voting-machine-security expert) ("It's possible to do a pretty good job of erasing all the forensic evidence.").

50. DeLuzio, *supra* note 47; McMillan & Volz, *supra* note 17 (noting that the National Academies of Sciences, Engineering, and Medicine recommended that "U.S. states move away from voting machines that don't include paper ballots").

constitutes a false equivalence to be resisted all the more mightily because of its subtle appeal.[51]

In short, paper ballots, whether manually counted or processed via optical-scan machines, provide a record of vote tallies independent from electronic capture and therefore are immune to electronic vote tampering, whether such tampering occurs at the polling place or from a remote location. Post-election audits conducted manually enjoy similar insulation from electronic vote tampering and therefore serve to increase public confidence in election outcomes.[52] Equally important, post-election audits can operate as a deterrent to fraud and corruption.[53]

Given the indispensable role audits play, the methods for their conduct merits scrutiny as well. Post-election audits come in a variety of flavors, two of which are relevant to this discussion: traditional and risk-limiting. The National Conference of State Legislatures reports that thirty-one states and the District of Columbia require "traditional" post-election audits, which review the ballots cast in a fixed percentage of voting districts or voting machines by "compar[ing] the paper record to the results produced by the voting system."[54] In a traditional post-election audit the number of ballots to be counted remains the same, regardless of the margin of difference between votes for a losing candidate and those for the winning candidate.[55] Depending on the jurisdiction, the traditional post-election audit may be conducted manually

51. Indeed, our current voting systems are in their current "distressed state," Zetter, *supra* note 16, in part, because the older, paper-based systems proved problematic during the 2000 presidential election—when the race in Florida required a recount, and the paper "butterfly ballots" and "hanging chads" made ascertaining voter intent all but impossible. Subsequently, many states—encouraged by Congress—transitioned to electronic voting machines as an improvement over the paper ballot systems. *Id.*

52. *Post-Election Audits*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 1, 2019), http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

53. *Id.* Post-election audits also act as a systemic corrective by alerting election officials of programming or other bugs or errors in the system. *Id.*

54. *Id.* (providing a 50-state survey of election-audit requirements).

55. *Id.* ("Even in a landslide election, [auditors] will count the same number of ballots as they would in a nail-biter election."). *Cf.* Schneider, *supra* note 37 ("With races involving wide margins, they can safely use relatively few samples. When the race is closer, it takes more samples to verify that the outcome is correct.").

in toto or in part, with some portion of the audit conducted electronically.[56]

A second type of post-election audit is the "risk-limiting" audit. Journalist Eric Geller explains how risk-limiting audits work as follows:

> In a risk-limiting audit, state officials select a sample of paper ballots—usually based on the margin of the outcome—and compare them using statistical methods to the electronically cataloged results of those ballots. They also select a "risk limit," which is the percentage chance that their audit will fail to catch incorrect results that could have been caused by tampering. For example, an audit with a risk limit of 5 percent will have a 95 percent chance of successfully catching the incorrect vote tabulation. Risk-limiting audits can be used to determine whether a more comprehensive recount is needed.[57]

In other words, risk-limiting audits use random sampling to "spot match[]" electronic and paper records, which allows "election officials [to] determine that the outcome is correct within a given risk level."[58]

For numerous reasons, experts increasingly recommend the risk-limiting audit.[59] First, and most importantly, the use of statistically sound sampling methods increases the reliability of the audits' results.[60] Of course, this in turn serves the imperative objective of enhancing public confidence in the accuracy of vote counts. Relatedly, post-election risk-limiting audits, when based on a paper-ballot record,

---

56. NAT'L CONFERENCE OF STATE LEGISLATURES, *supra* note 52.

57. Geller, *supra* note 42.

58. Schneider, *supra* note 37.

59. According to a recent consensus report produced by the National Academies of Sciences, Engineering, and Medicine, by 2028, "risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible." LINDEMAN, *supra* note 46, at 4 (citing NAT'L ACADS. OF SCI., ENG'G, & MED., *supra* note 46).

60. "Digital security specialists have long pushed for states to adopt risk-limiting audits, which they say are a fast and inexpensive way to give the public confidence that votes were not altered in any way." Geller, *supra* note 42.

"are robust enough to detect [vote-changing] cyberattacks,"[61] regardless of whether such cyberattacks originate from malign foreign actors or corrupt domestic ones.[62] Finally, risk-limiting audits are easy and inexpensive to administer.[63]

Despite the unequivocal recommendations of election and cybersecurity experts to adopt hand-marked paper ballots, auditable paper trails, and post-election risk-limiting audits, state election officials in most jurisdictions have thus far resisted making the recommended changes to their election and voting systems.[64] No doubt some combination of the failure to appreciate the gravity of the problem and bureaucratic inertia explains this inaction in part. But given the uncommon convergence of expert opinion and the salience of the issue, these causes seem so woefully inadequate as to spur speculation as to whether other impediments may be at work.

IV. COSTS AND CONFLICTS

Despite the stakes of ensuring both the accuracy of vote counting and the availability of risk-limiting audits as a robust mechanism for ensuring the same—not to mention demonstrated voter preference for paper ballots[65]—many election officials nevertheless have resisted

---

61. *Id.* (quoting J. Alex Halderman, University of Michigan computer science professor).

62. Most media attention devoted to electronic voting machine vulnerabilities focuses on threats from hostile foreign nations, but corrupt insiders can also wreak the same havoc. *See* Cohn, *supra* note 45 (quoting journalist Brad Friedman) (alteration in original) ("[Y]ou do not need to be a fancy state-sponsored hacking organization to do it. It's one guy on the inside, whether an election official, or a voting machine company, or contractor, or whatever . . . . It doesn't take a nation state to flip an election."); *see also* Bajak, *supra* note 43 ("No federal law requires [voting-machine vendors] to report security breaches or to perform background checks on employees or subcontractors.").

63. *See, e.g.*, Schneider, *supra* note 37 ("[R]isk-limiting audits are not particularly difficult or expensive to [implement]."); Geller, *supra* note 42 ("Risk-limiting audits are less expensive than other types of audits because they sample fewer ballots."); *see also infra* note 77 and accompanying text.

64. Halpern, *supra* note 1.

65. *See* Mark Niesse, *Georgia Panel Backs New Voting Machines Over Hand-Counted Paper Ballots*, ATLANTA JOURNAL-CONSTITUTION, https://www.ajc.com/news/state—regional-govt—politics/georgia-panel-backs-new-voting-machines-over-hand-marked-paper-ballots/feF5QiAwnzl2l3BK055dtI/ (last

adopting these measures. In this Part, we explore some of the possible explanations for this resistance.

A. Costs

Some jurisdictions lack the financial resources to upgrade aging voting machines and make the transition to voting systems that use voter-verifiable paper trails—ideally, hand-marked paper ballots—that can be audited.[66] When jurisdictions do have funding at their disposal, they have many options available, including electronic voting machines that are less expensive than those using paper ballots.[67] In addition, voting records must comply with federal retention requirements;[68] and paper records entail significantly greater storage costs than do electronic records. Finally, while risk-limiting audits are relatively inexpensive, they are not entirely free from cost, and a cash-strapped jurisdiction might be tempted to forgo them as unnecessary luxuries.

Of course, one potential source of funding for transitioning to paper ballots and conducting post-election audits is the federal government. In fact, election-security experts advocating for paper ballots and

updated Jan. 10, 2019) (describing "opposition from a crowd of voters who said paper ballots filled out by hand are more secure and less expensive"); Rich Garella, *High-Stakes Voting Machine Decision Deserves More Scrutiny*, PHILA. INQUIRER (Jan. 22, 2019, 7:01 AM), https://www.philly.com/opinion/commentary/philadelphia-voting-machines-city-commissioners-20190122.html (explaining that hand-marked ballots are "the preferred choice of election security experts and the overwhelming majority of those [voters] who attended the [City Commission] hearings [on the selection of a new voting system]").

66. Buchanan & Sulmeyer, *supra* note 18, at 14 ("Severe funding shortfalls prevent the updating of voting machines and means that they are often used well past their intended use date."); Wogan, *supra* note 37 ("Lack of funding is the main reason some states don't have paper [ballots].").

67. More expensive electronic voting machines are also available. We discuss below possible reasons why elections officials select the more expensive electronic voting machines over the more affordable paper ballots. *See* discussion *infra* Section IV.B.1.

68. 52 U.S.C. § 20701 (2012) (setting forth a twenty-two month retention period for ballots in any election for candidates for federal office).

paper-trail audits recently called on Congress to make such funding available to states to upgrade their voting and auditing systems.[69]

Even when the costs of paper ballots are lower than those for electronic ballots, however, election officials have demonstrated a preference for the latter.[70] This resistance is somewhat puzzling at first blush in light of the emphatic and uniform consensus among election-security experts that paper ballots and post-election paper-trail audits—and in particular risk-limiting audits, which require paper voting records[71]—serve as the gold standard for ensuring accurate vote tallies.[72] What could explain such reticence when expense is no longer an objection?

B. Conflicts of Interests (and Their Appearance)

Motives far stronger than cost concerns may in some instances explain a state's resistance to adopting best practices. Personal interests, whether financial or political, may distort decisions about con-

69. Buchanan & Sulmeyer, *supra* note 18, at 17 ("Additional funding for a voter-verifiable paper trail in all future elections is essential as a bulwark against perceptions of a hacked result."); Geller, *supra* note 42 ("A coalition of experts recently urged lawmakers to give states money to upgrade their technology so they can adopt the necessary procedures."). Congress has previously provided funding for upgrading voting machines through the Help America Vote Act and recently introduced a bill that would, among other things, create grants to states for conducting audits of election results. *See* Tim Lau & Daniel I. Weiner, *Historic Bill to Strengthen Democracy Introduced in Congress*, BRENNAN CTR. FOR JUST. (Jan. 3, 2019), https://www.brennancenter.org/blog/historic-bill-strengthen-democracy-introduced-congress (providing a synopsis of H.R. 1 "For the People Act").

70. *See* Garella, *supra* note 65 (describing Philadelphia as being on the cusp of choosing an electronic system); Halpern, *supra* note 1 (noting that the following states and counties either had selected electronic systems or were poised to do so: Georgia, Delaware, and counties in Ohio, Kansas, New Jersey, and Arkansas); *see also infra* note 77 and accompanying text.

71. "Access to paper voting records is essential for risk-limiting audits." Schneider, *supra* note 37 (quoting Colorado's Secretary of State Wayne Williams) ("You have to have paper ballots that you can actually audit . . . . Something a voter can verify. And then after the election we randomly select ballots from across every single polling place, every single voter, and every single county . . . to audit a certain number of ballots.").

72. Geller, *supra* note 42.

tracting with voting-machine vendors, vendor oversight, and the conduct of post-election audits. We document below cause for such concerns.

1. Vendor Contracting and Oversight

Given all that is at stake, governmental decisions relating to the purchase of electronic voting machines and oversight of their operation need to be based solely on the public's interests in efficiency and, especially, reliability. But these devices' provision and operation are the result of a marketplace in which vendors compete for governmental favor, possibly in ways that have little to do with the public interest. Officials charged with purchasing and oversight authority may be distracted by self-interest manifest in such familiar forms as campaign contributions to those holding elected positions, as many do, or in "revolving door" relationships with potential vendors.[73] Not only might such distractions distort purchase decisions, but they may also compromise the rigor of governmental assessment of vendors' commonplace claims that their proprietary interests in their own hardware and software preclude independent post-election forensic analysis of the vote

73. "The voting-machine industry—an estimated $300-million-a-year business—has long been as troubling as the machines it makes, known for its secrecy, close political ties (overwhelmingly to the Republican Party)[,] and a revolving door between vendors and election offices." Zetter, *supra* note 16. For example, a search of the donor database of the Nevada Secretary of State Financial Disclosure Statements documenting political contributions disclosed that vendor Election Systems & Software ("ES&S") donated at least $32,500 between 2013 and 2016 to the Republican State Leadership Committee ("RSLC"). *See Aurora Campaign Finance Disclosure*, NEV. SEC'Y OF STATE, https://www.nvsos.gov/SOSCandidateServices/AnonymousAccess/CEFDSearchUU/Search.aspx (last visited Mar. 16, 2019) (select "Contribution Search" under the "Search Type" menu; then search "Election Systems & Software"). According to the RSLC's website, the organization's stated mission is "to elect Republicans to down-ballot, state-level offices." *See* REPUBLICAN STATE LEADERSHIP COMMITTEE, https://rslc.gop/ (last visited Mar. 16, 2019). Reporter Jane Mayer refers to the RSLC as "a catchall bank account for corporations interested in influencing state laws." JANE MAYER, DARK MONEY: THE HIDDEN HISTORY OF THE BILLIONAIRES BEHIND THE RISE OF THE RADICAL RIGHT 243 (2016). For a detailed account of the "revolving door" phenomenon in Georgia since 2002, see Halpern, *supra* note 1.

tallies they produce.[74] Similarly, conflicts of interest may cause governmental bodies charged with overseeing elections to be lax in requiring best practices for election security.[75]

For evidence that concerns about conflicts of interest are not merely speculative, one need look no further than the recent decision by Georgia's Secure Accessible and Fair Elections ("SAFE") Commission, which voted in January to replace the State's electronic voting machines with a new computerized system that prints paper ballots.[76] In doing so, the SAFE Commission rejected pleas for the use of substantially less expensive hand-marked paper ballots backed by best-practices advice from election cybersecurity experts—including the one expert appointed to the panel—as well as all voter comments at a public hearing.[77]

Though well-named, the SAFE Commission acted in circumstances unfortunately giving ample reason to doubt the independence of the Commission's judgment. Populated by then-Secretary of State Brian Kemp, the SAFE Commission cast its final vote the same week that Kemp, in his new capacity as Governor-elect, announced his appointment of a lobbyist for Election Systems & Software ("ES&S") as his deputy chief of staff.[78] ES&S happens to sell the kind of machines, expected to cost the State approximately $100 million, that the SAFE

74. *See* Cohn, *supra* note 45 ("[M]achine vendors claim proprietary ownership of their software and hardware, precluding [post-election] forensic analysis."); *see also* Bajak, *supra* note 43 ("Election vendors have long resisted open-ended vulnerability testing by independent, ethical hackers—a process that aims to identify weaknesses an adversary could exploit. Such testing is now standard for the Pentagon and major banks.").

75. According to journalist Frank Bajak, for example, "California, New York, and Colorado are among states that tend to keep a close eye on the vendors. States with cozier relationships have in the past let them use remote-access software to do maintenance on election systems, a widely discredited security [practice]." Bajak, *supra* note 43 (as reprinted in CHRISTIAN SCIENCE MONITOR, Oct. 29, 2018).

76. Niesse, *supra* note 65. The SAFE Commission's vote (13-3 in favor of the new system) is non-binding, but it is expected to guide the final vote by the Georgia legislature when that body takes up the issue later this year. *Id.*

77. *Id.* The recommended voting system would cost over $100 million; whereas a paper ballot system would cost approximately $30 million. *Id.*

78. *Id.* The panel enjoyed a less than auspicious origin in that, as we detail below, Kemp—in his capacity as Secretary of State—oversaw his own gubernatorial election. *See infra* text accompanying notes 100–07.

Commission recommended.[79] The SAFE Commission's recommendation of that ES&S system, known as "ExpressVote," came on the heels of Kemp's invitation to ES&S in August 2017 to operate a pilot version of the ExpressVote system in a municipal election in Rockdale County, Georgia.[80] According to election-technology experts, voting-systems vendors that implement such pilot projects secure more than simply a competitive advantage when lawmakers ultimately dictate the terms for voting-systems purchases by election officials; voting-systems vendors can also effectively establish the requirements for such purchases by persuading legislators to structure particularized calls for vendor bids so that only one vendor's products will meet the requirements.[81]

ES&S's influence over state election officials' voting-systems decision-making is limited neither to Georgia nor to the administration of pilot projects. For example, since 2009, ES&S has convened what it calls an "advisory board"—comprised of a small number of state election officials—and regularly provided the advisory board with trips to vacation destinations, such as New York and Las Vegas, which also included the costs of airfare, high-end accommodations, and live-entertainment tickets.[82] As for the influence ES&S wields in other states, consider that "last fall in Delaware . . . the Voting Equipment Selection Task Force . . . voted to replace its aging touch-screen machines with a variant of the ExpressVote system."[83] A government accountability watchdog group "obtained all the bids from a public-records request," and found that "the Department of Elections had pretty much tailored the request for [bids] in a way that eliminated vendors whose primary business was to sell paper-ballot systems."[84] The watchdog group spokesperson noted that an ES&S lobbyist with close connections within the State had shepherded the selection process that resulted in the selection of the ES&S system.[85] Similarly, individual counties across the nation have chosen to adopt the ES&S ExpressVote system

79. Niesse, *supra* note 65.

80. Halpern, *supra* note 1.

81. *Id.*

82. *Id.*

83. *Id.*

84. *Id.* (describing efforts by Common Cause Delaware to review bids by voting machine vendors for state contracts).

85. *Id.*

in the past year.[86] Philadelphia seems poised to follow suit.[87] Membership on the ES&S Advisory Board raises concerns about election officials' conflicts of interest and the appearance of conflicts in several voting precincts in various states, including the Executive Director of the South Carolina Election Commission;[88] the Elections Director for Luzerne County, Pennsylvania;[89] and the Director of the Board of Elections of New York City.[90]

Such conflicts of interest (or the appearance of such conflicts) raise serious concerns that should be addressed to ensure that the electoral systems and processes that are used are not only trustworthy, but also that they are trusted.[91] In other words, it matters little whether such systems are in fact trustworthy if citizens do not trust that they will produce accurate outcomes because such lack of trust undermines public faith in democratic institutions. Whatever may be state election officials' motives, any reluctance on their part to ensure the integrity and

86. *Id.* (listing counties in Ohio, Kansas, New Jersey, and Arkansas). At least one state has defended its choice to resist the use of paper ballots by saying that voters are already familiar with electronic voting systems, and that the new machines do not constitute major changes. *See id.* ("Elaine Manlove, the Delaware elections director, [stated] . . . 'It's not a big change for Delaware voters' . . . . 'They're voting on the screen, just like they do now.'").

87. Garella, *supra* note 65.

88. Andrew Brown, *SC Election Director's Ties to Voting Company Creates 'Conflict' Concerns*, POST AND COURIER (Jan. 29, 2019), https://www.postandcourier.com/news/sc-election-director-s-ties-to-voting-company-creates-conflict/article_60e83cd2-23ee-11e9-bc66-4711ed41504e.html.

89. Eric Mark, *County Election Official in Conflict of Interest?*, CITIZENS' VOICE (Dec. 6, 2018), https://www.citizensvoice.com/news/county-election-official-in-conflict-of-interest-1.2418774.

90. Denis Slattery, *NYC Board of Elections Boss Didn't Properly Report Lavish Trips Funded by Voting Machine Company*, N.Y. DAILY NEWS (Dec. 4, 2018, 9:25 AM), https://www.nydailynews.com/news/politics/ny-pol-boe-head-michael-ryan-trips-voting-machine-company-20181204-story.html.

91. *See* Letter from Former United States President Jimmy Carter, to then-Secretary of State for the State of Georgia Brian Kemp (Oct. 22, 2018), *in Full Text of Carter's Letter to Georgia Secretary of State*, ASSOCIATED PRESS (Oct. 29, 2018) [hereinafter Letter from President Carter], https://www.apnews.com/02bf11f29ada46d0833be6e3091b0c31 ("In order to foster voter confidence in the upcoming election, which will be especially important if the race ends up very close, I urge you to step aside and hand over to a neutral authority the responsibility of overseeing the governor's election.").

reliability of voting machines and systems within the scope of their responsibility comes at a serious cost to voter confidence. Presently, the federal government does little in the way of oversight to act as a stopgap—whether by, for example, testing machines, software, or systems for security vulnerabilities;[92] accrediting vendors;[93] or requiring the reporting of security breaches.[94] Moreover, no oversight exists to protect against personnel security risks, such as requiring vendors or their subcontractors to conduct background checks on employees.[95]

In the absence of federal oversight, state and local election officials are responsible for identifying and remediating vulnerabilities in the nation's voting machines and systems.[96] With a handful of exceptions,[97] states have not proven themselves up to the task. For example, the *Wall Street Journal* reported that "[e]lection machines [manufactured by one of the three major vendors] [and] used in more than half of U.S. states carry a flaw disclosed more than a decade ago that makes

92. In some voting districts, for example, "vendors and contractors are involved in every phase of elections, from writing the software that registers voters and determines their eligibility to cast ballots, to programming machines and counting the votes. And it's not clear to what degree, if any, they're subject to oversight." Zetter, *supra* note 16.

93. Bajak, *supra* note 43.

94. *Id.*

95. As Frank Bajak explains:

> At the federal level, no authority accredits election vendors or vets them or their subcontractors. . . . Federal oversight is limited to the little-known Election Assistance Commission, a 30-employee agency that certifies voting equipment but whose recommendations are strictly voluntary. It has no oversight power and cannot sanction manufacturers for any shortcomings.

Id.

96. DeLuzio, *supra* note 47 ("Remarkably, there is no federal regulatory regime governing election vendors, which perform many critical election-related functions, such as ballot preparation, logic and accuracy testing, and equipment manufacturing and servicing. This regulatory vacuum puts the onus on state and local officials to closely scrutinize vendors for cybersecurity-related risks and to assess vulnerabilities in vendors' supply chains.").

97. Most notably, in 2009, Colorado adopted paper ballots and risk-limiting audits. Geller, *supra* note 42.

them vulnerable to a cyberattack."[98] Yet, to date, those flaws have largely remained unaddressed.[99]

2. Audit Authorization and Supervision

Decisions about the necessity for and adequacy of post-election audits are often made by public officials who, in addition to the kinds of financial motives arising from campaign contributions or "revolving door" professional opportunities, may also be improperly influenced by partisan political incentives. Most starkly, an elected official who is a candidate in an election may be entrusted by law with control over the decision about whether to order a post-election audit of that same election. In 2018, then-Secretary of State for the State of Georgia, Brian Kemp, drew criticism for his dual role as gubernatorial candidate and top state election official in an exceedingly close race that Kemp eventually won amid numerous instances of irregularities, both before and on election day.[100] In this case, a full audit, however compelling the case may have been for one, was not possible even assuming that Kemp would have been inclined to conduct one because Georgia is one of five states that uses touchscreen electronic voting machines that provide no paper record or paper-ballot backup.[101] But as the election's winner, Kemp also had a powerful personal motive for avoiding an audit, as it was in his own political interest for the vote tally to remain unexamined and unchanged.

Former President Jimmy Carter voiced these concerns in an open letter to then-candidate Kemp, urging him to resign his position as Secretary of State so that he would no longer be overseeing his own election.[102] President Carter wrote, "one of the key requirements for a fair and trusted process is that there be nonbiased supervision of the electoral process" and emphasized the need to "eliminate concerns about a conflict of interest . . . . to ensure the confidence of our citizens

98. McMillan & Volz, *supra* note 17.

99. *Id.*; *see also* Cortes & Norden, *supra* note 44.

100. Emily Dreyfuss, *Georgia Voting Machine Issues Heighten Scrutiny on Brian Kemp*, WIRED (Nov. 6, 2018, 4:54 PM), https://www.wired.com/story/georgia-voting-machine-issues-heighten-scrutiny-brian-kemp.

101. *Id.*

102. Letter from President Carter, *supra* note 91.

on the outcome."[103] President Carter's focus on "the most fundamental principle of democratic elections—that the electoral process be managed by an independent and impartial election authority" applies equally to all public officials with the responsibility for selecting and managing voting machines and systems, including post-election audits.[104]

Brian Kemp was not the only official recently overseeing an election in which he was also a candidate. In Florida, in 2016, then-Governor Rick Scott, who was running for (and ultimately won) a United States Senate seat, bowed to pressure—brought to bear in part by a lawsuit filed against him—to recuse himself from certifying his own election results.[105] And in Kansas, then-Secretary of State Kris Kobach oversaw the bulk of the primary election in his bid for Governor, recusing himself only after his primary victory was secure.[106]

Actual conflicts, such as a public official overseeing his or her own election or post-election certification, pose clear problems for public perceptions of election-outcome legitimacy. That is, voters will be less likely to trust an electoral race's outcome if the public official overseeing or certifying the election has a stake in the results. This is especially true if elections involve irregularities in voting accessibility or vote tallying, and even more so when, as occurred in Georgia, the official overseeing the election also engaged in multiple, demonstrable efforts to suppress the vote among those more likely to vote for his opponent.[107]

---

103. *Id.*

104. *Id.*; s*ee also* Sue Halpern, *How Voting-Machine Errors Reflect a Wider Crisis for American Democracy*, NEW YORKER (Oct. 31, 2018), https://www.newyorker.com/news/news-desk/how-voting-machine-errors-reflect-a-wider-crisis-for-american-democracy ("If the state's voting machines . . . are flipping [votes] in his favor, there will be no way to prove it.").

105. Carney, *supra* note 24.

106. Carney, *supra* note 24 (Kobach ultimately lost the general election).

107. Richard L. Hasen, *Brian Kemp Just Engaged in a Last-Minute Act of Banana-Republic Level Voter Manipulation in Georgia*, SLATE (Nov. 4, 2018, 3:47 PM), https://slate.com/news-and-politics/2018/11/georgia-governor-candidate-brian-kemp-attempts-last-minute-banana-republic-style-voter-manipulation.html (describing Kemp's false accusations that the Democratic Party had hacked into the State's database); Carol Anderson, *Brian Kemp's Lead in Georgia Needs an Asterisk*, THE

But even the mere appearance of conflicts—such as when the public officials responsible for selecting or recommending voting machines accept "lavish" trips fully funded by the vendors of those same machines—can undermine the public trust in election outcomes. Voters' trust in election outcomes will be more likely to erode where such officials buck both cybersecurity or election-integrity experts' recommendations and voters' preferences by selecting vendor-promoted machines that are also more vulnerable to tampering by malign actors.

The risks are especially grave now, in an age when malign actors seek to disrupt and delegitimize not only individual elections, but also democratic institutions by exploiting vulnerabilities in electoral systems and manipulating voter trust. Both actual conflicts and the appearance of conflicts are ripe for exploitation. Furthermore, voting precincts that do not use paper ballots and require paper-record post-election audits substantially exacerbate risks because any irregularities resulting in a tainted vote count are harder to detect.[108]

Public confidence in voting systems serves as an indispensable feature of a full and healthy democracy, and conflicts of interest or, at least, the appearance of conflicts of interest operate to erode public

---

ATLANTIC (Nov. 12, 2018), https://www.theatlantic.com/ideas/archive/2018/11/georgia-governor-kemp-abrams/575095/ (drawing attention to Kemp's purges of voter rolls, closure of polling locations, and blocking of voter registrations).

108. Bajak, *supra* note 43 (reporting that, despite no evidence of hackers penetrating vulnerable electronic voting machines preceding the 2018 midterm elections, "authorities acknowledge that some election mischief or malware booby traps may have gone unnoticed"); Jennifer Cohn, *Despite Apparent Conflict of Interest, Georgia's SAFE Commission Is Poised to Recommend a New Touchscreen Barcode Balloting System that Will Cost Taxpayers More Than Three Times as Much as Hand Marked Paper Ballots & Scanners, While Providing Less Security*, MEDIUM (Dec. 11, 2018), https://medium.com/@jennycohn1/despite-apparent-conflict-of-interest-georgias-safe-commission-is-poised-to-approve-a-new-ba6f683c3727 (noting that Georgia does not require manual, post-election audits); Cortes & Norden, *supra* note 44 (noting that, if a malign actor tampers with paperless voting machines, "there is no record independent of the software (e.g., a paper ballot) that can be used to check the results"); Jack Gillum & Jeff Tao, *File-Sharing Software on State Election Servers Could Expose Them to Intruders*, PROPUBLICA, (Nov. 2, 2018, 5:00 AM), https://www.propublica.org/article/file-sharing-software-on-state-election-servers-could-expose-them-to-intruders (criticizing the use of FTP service to report election results as insecure and explaining that "malicious attackers can change the contents of a transmission without either side detecting the change").

trust.[109] "The practice of democracy begins with casting votes; its integrity depends on the inclusivity of the franchise and the accurate recording of its will."[110] When the public believes that voting tallies may have been tainted—regardless of that belief's accuracy—then not only may the public doubt the legitimacy of the outcome itself, but the electorate is also less likely to trust in the validity of the laws enacted by candidates who were selected under the tainted (or perceived-to-be-tainted) election. Moreover, when the very public officials whose job is to ensure voting tallies' accuracy are the same ones who refuse to take transparent action to ensure voting tallies' reliability, and that refusal takes place under the shadow of conflicts of interest or an appearance of conflicts of interest, then both the decision maker's motives and the voting tallies' legitimacy fall under greater suspicion. In short, by crippling public confidence, conflicts of interest—whether perceived or real—weaken critical democratic institutions.

3. Restoring Trust: Looking to the Law of Trusts

So, the question becomes: how should we address conflicts of interest (whether financial or political) of government officials whose responsibility is to select and employ reliable and secure voting machines and systems that produce accurate and transparent vote counts? One powerful lens through which to understand—and potentially address—this question is the public fiduciary theory.[111]

In both private law and public ethics law, the fiduciary principle operates to prevent individuals holding positions of responsibility from using those positions in their own self-interest.[112] As "[t]he antithesis of conflicts of interest," the fiduciary principle requires all conflicting

---

109. Buchanan & Sulmeyer, *supra* note 18, at 15 (noting that even "[t]he perception of illegitimacy is damaging").

110. Halpern, *supra* note 1.

111. *See* Kathleen Clark, *Do We Have Enough Ethics in Government Yet? An Answer from Fiduciary Theory*, 1996 U. ILL. L. REV. 57, 74 (1996) ("Numerous courts have recognized the fiduciary obligation of government employees, even in the absence of specific legislative or regulatory endorsements of such duties, and these courts have imposed fiduciary-like remedies in response to violations of the conflict and influence components of that obligation."); *see also* Hill & Painter, *supra* note 7, at 1644 (observing that "[o]fficials in all branches of government owe fiduciary obligations to the public").

112. Hill & Painter, *supra* note 7, at 1644.

interests held by persons entrusted with a position of responsibility to be resolved in favor of the "interests of those persons [owed] fiduciary duties, preferring those interests to any other interests."[113]

Elsewhere we have argued that the fiduciary tenets governing the law of private trusts should form the basis for remedial measures in the enforcement of the Constitution's anti-corruption mechanisms set forth in the Foreign and Domestic Emoluments Clauses.[114] Here, we contend that the fiduciary precepts from the private law of trusts can—and should—serve as guideposts for understanding public officials' conflicts of interest in the context of selecting voting systems and tallying election votes. These same conflicts also operate as a broader betrayal of the electorate's trust by failing to ensure that the selected voting machines and systems are secure, reliable, and accurate. By way of cascading effects, they in turn undermine principles of good governance, including public trust in electoral outcomes.[115] More generally, we argue that the core fiduciary tenet of the duty of loyalty owed by a trustee to a beneficiary should inform how voters, legislators, courts, legal scholars, and advocates of free and fair elections evaluate the decisions by office-holders concerning electoral and post-election systems and processes.

The duty of loyalty imposes the unyielding requirement that the trustee act solely in the best interests of the beneficiary.[116] When public

---

113. *Id.*

114. *See* Breedon & Bryant, *The Brand v. The Man: Considering a Constructive Trust as a Remedy for President Trump's Alleged Violations of the Foreign Emoluments Clause*, *supra* note 3; Breedon & Bryant, *The Potential Roles of the Constructive Trust and the Blind Trust as Remedies for Emoluments Clause Violations*, *supra* note 2.

115. Corruption is generally recognized as an impediment to good governance and is frequently associated with anti-democratic, autocratic systems. Zoe Pearson, *An International Human Rights Approach to Corruption*, *in* CORRUPTION AND ANTI-CORRUPTION 41 (Peter Larmour & Nick Wolanin eds., 2001). Practices of good governance include, for example, "[the] recognition of fundamental human rights, [the observance of] the rule of law, [the] strengthening of institutions, [the promotion of] political participation[,] and [the] strengthening of civil society and democracy." *Id.*

116. A CONCISE RESTATEMENT OF DONATIVE TRANSFERS AND TRUSTS § 78, at 769 (THOMAS P. GALLANIS, ed. 2017). "The duty of loyalty is, for trustees, particularly strict even by comparison to the standards of other fiduciary relationships." *Id.*, cmt. a, at 770. This fiduciary obligation is one of undivided loyalty to the beneficiaries

officials make decisions that are not solely in the interest of the people, the people may be wrongly deprived of public resources; stripped of procedural protections; or denied substantive rights, including basic human and political rights.[117] Additional potential consequences flowing therefrom include the rise of cynicism among the electorate and a diminished (or extinguished) faith in democratic institutions.[118] All these outcomes pose potential risks to democratic self-governance.[119] These risks are, we believe, all the more grave when the institution suffering from public corruption or conflicts of interest is the electoral system itself.

When voters are given cause to be concerned about the integrity of the electoral systems they use to cast their ballots or the accuracy of the vote tally, any conflicts of interest among public officials entrusted with the responsibility to ensure electoral integrity and voting accuracy serve not only to heighten voters' concerns about the outcome of the specific race (or races) at issue, but also about the legitimacy of democratic self-governance more broadly.[120] In her recent opinion in *Curling v. Kemp*, an on-going action alleging Brian Kemp violated the Fourteenth Amendment's Equal Protection and Due Process Clauses in the

---

and requires the trustee to "subordinate his own interests to the welfare of the beneficiaries" in all matters pertaining to the trust. Robert G. Natelson, *The Constitution and the Public Trust*, 52 BUFF. L. REV. 1077, 1089 (2004) (citations omitted).

117. Pearson, *supra* note 115, at 52–58; Stockmeyer et al., *supra* note 16, at 82 ("Corruption . . . undermines good governance, the rule of law, economic development, and moral values . . . [and] also hinders citizens' participation in elections.").

118. Pearson, *supra* note 115, at 50; Stockmeyer et al., *supra* note 16, at 82 (finding "statistically significant and substantively relevant negative impact" of corruption on voter turnout). Stockmeyer concludes: "Confronted with mediocre governance performance, citizens in corrupt democracies may be unwilling or unable to establish trustworthy relations with their representatives. As a result, citizens may distance themselves from the political system, preferring to stay home on election day." Stockmeyer et al., *supra* note 16, at 84.

119. Stockmeyer et al., *supra* note 16, at 83–84 ("Corrupt practices not only hinder economic and social development, they also prevent democracies from functioning properly."); *see also* Brief of Amica Curiae Sarah P. Chayes in Support of Plaintiffs, Citizens for Responsibility & Ethics in Washington v. Trump, No. 17 Civ. 00458 (GBD), 2017 WL 7795995 (S.D.N.Y.).

120. *See* Stockmeyer et al., *supra* note 16, at 78 (concluding that corruption likely "has a more severe impact in democracies" because it "undermines democratic institutions and decreases individuals' trust in politicians").

recently concluded Georgia gubernatorial election, Judge Amy Totenberg reflected these broader effects: "A wound or reasonably threatened wound to the integrity of a state's election system carries grave consequences beyond the results in any specific election, as it pierces citizens' confidence in the electoral system and the value of voting."[121] Judge Totenberg further noted the importance of voting systems in "address[ing] democracy's critical need for transparent, fair, accurate, and verifiable election processes that guarantee each citizen's fundamental right to cast an accountable vote."[122]

Trust in election integrity in the United States has taken a hit in recent years. In an NPR/Marist poll conducted shortly before the 2018 midterm elections, almost half of the respondents indicated that they did not fully trust that their votes would be counted accurately.[123] In recognition of the need in a healthy democracy for elections to be both trustworthy and trusted, some members of Congress have sought to address vulnerabilities and bolster public confidence.

V. LEGISLATION AND (TO DATE) LETHARGY

In the aftermath of the 2016 elections, and amid still-ongoing concerns about cyberattacks on our election and voting systems by Russian military computer hackers, several members of Congress introduced legislation aimed at minimizing the potential for hostile actors to interfere with our nation's electoral systems. Between the House and the Senate, at least six bills were introduced in the last two years addressing election security: House Bill 6188, the "Prevent Election Hacking Act of 2018";[124] House Bill 6093 and Senate Bill 3049 (companion bills with identical language in the House and the Senate), both called the "Protecting American Votes and Elections Act of 2018"

121. Curling v. Kemp, 334 F. Supp. 3d 1303, 1328 (N.D. Ga. 2018).

122. *Id.*

123. Miles Parks, *NPR/Marist Poll: 1 in 3 Americans Thinks A Foreign Country Will Change Midterm Votes*, NPR (Sept. 17, 2018, 5:00 AM), https://www.npr.org/2018/09/17/647420970/npr-marist-poll-1-in-3-americans-think-foreign-country-will-change-midterm-votes (finding that in the months before the 2018 federal elections, nearly 40% of Americans doubted election security from foreign interference); Schneider, *supra* note 37.

124. Prevent Election Hacking Act of 2018, H.R. 6188, 115th Cong. § 1 (2018).

("the PAVE Act");[125] and House Bill 6663 and Senate Bill 2261 (bills with similar—but not identical—language in the House and the Senate), both called the "Secure Elections Act."[126] In January 2019, the House introduced a comprehensive election integrity, election security, and anti-corruption bill, House Bill 1, the "For the People Act of 2019."[127]

The Prevent Election Hacking Act of 2018 directs the Department of Homeland Security to create a "bug bounty" program, the purpose of which is to encourage election officials at the state and local levels and election service providers to work with independent technical experts in identifying "previously unidentified election cybersecurity vulnerabilities."[128] As conceived, this "Hack the Election" program makes participation by election officials and election service providers "entirely voluntary."[129] Introduced in the House on June 21, 2018, House Bill 6188 was referred to the Committee on House Administration.[130] As of this writing, no further action has been recorded on this bill, though the "bug bounty" concept also makes an appearance in the For the People Act of 2019, discussed in more detail below.

The PAVE Act, introduced in the House and the Senate as companion bills in June 2018, would require the use of paper ballots and post-election risk-limiting audits for all federal elections.[131] In its findings section, the proposed PAVE Act emphasizes the twin goals that elections be both trustworthy and trusted.[132] As a basis for requiring paper ballots, Section 2 states: "Access to the ballot, free and fair elections, and a trustworthy election process are at the core of American

125. Protecting American Votes and Elections Act of 2018, H.R. 6093, 115th Cong. (2018); Protecting American Votes and Elections Act of 2018, S. 3049, 115th Cong. (2018).

126. Secure Elections Act, H.R. 6663, 115th Cong. (2018); Secure Elections Act, S. 2261, 115th Cong. (2018).

127. For the People Act, H.R. 1, 116th Cong. (2019).

128. H.R. 6188, § 2(c)(3), (e).

129. *Id.* § 2(b)(1).

130. H.R. 6188.

131. Protecting American Votes and Elections Act of 2018, H.R. 6093, 115th Cong. § 2(1)–(3) (2018); Protecting American Votes and Elections Act of 2018, S. 3049, 115th Cong. § 2(1)–(3) (2018).

132. H.R. 6093, § 2(1)–(3); S. 3049, § 2(1)–(3).

Democracy."[133] Similarly, as a reason for requiring post-election risk-limiting audits, Section 2 provides: "This will ensure that Americans have confidence in their election results."[134] Although the bill provides funding for ensuring accessibility for disabled voters,[135] it does not authorize funding to help states cover the costs of transitioning to paper-record elections or for administering risk-limiting audits. In the House, the bill was referred to the Committee on House Administration and to the Committee on Science, Space, and Technology.[136] In the Senate, it was referred to the Committee on Rules and Administration.[137] None of the three committees in either chamber has moved the bill forward as of this writing.

The Secure Elections Act, as introduced in both chambers of Congress, states that its goal is "[t]o protect the administration of [f]ederal elections against cybersecurity threats."[138] As introduced in the Senate, in December 2017, the bill would require, among other things, paper ballots and post-election audits by tabulating "a random sample of the marked paper ballots" so as to "establish high statistical confidence in the election result."[139] The bill would provide funding to assist states in complying with standards relating to the "procur[ement], maint[enance], testing, auditing, operating, and updating [of] election systems,"[140] to be developed by an advisory panel created under a separate provision of the bill.[141] Any remaining funds from such a grant could—with the approval from the Secretary of the Department of Homeland Security—be applied toward "improv[ing], upgrad[ing], or acquir[ing] hardware, software, or services related to election administration consistent with [those guidelines]."[142] None of the grant money, however, may be used "for any voting system that records each vote in electronic storage unless the system is an optical scanner that

133. H.R. 6093, § 2(1); S. 3049, § 2(1).

134. H.R. 6093, § 2(3); S. 3049, § 2(3).

135. H.R. 6093, § 4; S. 3049, § 4.

136. *See* H.R. 6093.

137. *See* S. 3049, § 2(1)–(3).

138. Secure Elections Act, H.R. 6663, 115th Cong. (2018); Secure Elections Act, S. 2261, 115th Cong. (2018).

139. S. 2261, § 5(d).

140. *Id.* § 5(b)(1).

141. *Id.* § 7(c).

142. *Id.*

reads paper ballots."[143] The bill was referred to the Committee on Rules and Administration, which held hearings on it in June 2018.[144] Soon thereafter, however, the White House, vendors' lobbyists, and state Secretaries of State voiced objections, and the bill lost support among several Senators.[145] Among the reasons for objecting to the bill were concerns about federalism and the requirement that voting systems use only paper ballots.[146] As a consequence of these objections, the Senate version of the Secure Elections Acts has stalled in committee.[147]

Apparently in response to the concerns raised regarding the Senate version of the Secure Elections Act, the House introduced a similar bill that incorporated language more protective of states' interests. The House version of the Secure Elections Act (H.R. 6663) opens with a "sense of the Congress" statement: "the States conduct elections and should maintain control of and responsibility for them" and "it is important to maintain State leadership in election administration."[148] Although this version also provides grant money for states to acquire and use voting machines that provide a paper record and to conduct post-election audits, it (unlike the Senate version) does not require paper

143. *Id.*

144. The official governmental website for information on federal legislative information, https://www.congress.gov, lists June 20, 2018, as the last date on which the Committee on Rules and Administration held hearings or otherwise took action on this bill. CONGRESS.GOV, S.2261—SECURE ELECTIONS ACT, https://www.congress.gov/bill/115th-congress/senate-bill/2261/actions?q=%7B%22search%22%3A%5B%22%5C%22Secure+Elections+Act%5C%22%22%5D%7D&r=3&s=2 (last visited Mar. 16, 2019).

145. Derek Hawkins, *The Cybersecurity 202: Why the Latest Election Security Bill Is Stalled in Congress*, WASH. POST (Aug. 31, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/08/31/the-cybersecurity-202-why-the-latest-election-security-bill-is-stalled-in-congress/5b8829fb1b326b3f31919eaa/?utm_term=.27f880733bfa; Derek B. Johnson, *Senators Duel Over Audit Requirements in Election Security Bill*, FED. COMPUTER WK. (Aug. 21, 2018), https://fcw.com/articles/2018/08/21/election-paper-ballots-bill.aspx (reporting that comments from some senators indicated "that state election officials and voting machine manufacturers have been putting increasing pressure on lawmakers to water down the bill").

146. *See* Hawkins, *supra* note 145; Johnson, *supra* note 145.

147. *See* CONGRESS.GOV, *supra* note 144.

148. Secure Elections Act, H.R. 6663, 115th Cong. § 2(1)–(2) (2018).

ballots, though it does require a paper record for post-election auditing.[149] The House version also allows grant money to be used for "a voting system with an electronic user interface."[150] In addition, as in the Senate version, the House version specifies that a state may qualify for grants to help the state comply with election cybersecurity guidelines to be established by an advisory panel constituted under a separate section of the bill.[151] Similarly, leftover funds from such a grant could be used "to improve, upgrade, or acquire hardware, software, or services for the purposes of improving administration of Federal elections, consistent with [those] guidelines," as long as certain requirements are met, including obtaining the approval of the Election Assistance Commission (as opposed to the Secretary of the Department of Homeland Security, whose approval would be required by the Senate bill).[152]

As its first priority in 2019, the House introduced the For the People Act, a sweeping elections and anti-corruption bill. The bill's provisions include a multi-pronged framework for "ensur[ing] that American elections are decided by American voters without interference by enhancing federal support for voting system security, particularly paper ballots; increasing oversight over election vendors; and requiring the development of a national strategy to protect U.S. institutions."[153] More specifically, the For the People Act—among other things—requires the use of paper ballots;[154] imposes a ban on

149. *Id.* § 5(d)(1)–(2). The House version therefore provides weaker protection against possible vote tampering than does the Senate version. As noted above, see *supra* text accompanying notes 38–43 and notes 40–41, some electronic touchscreen voting machines that register votes digitally provide a printable paper record, sometimes as barcodes, and those paper records can (technically) be used to audit the digitally registered vote. But cybersecurity experts agree that audits based on this type of paper trail are more difficult and less reliable than those based on voter-marked paper ballots, which are immune to electronic tampering.

150. H.R. 6663, § 7(f)(2).

151. *Id.* § 7(b)(1)(C); *cf.* S. 2261, § 7(c)(1).

152. *Compare* H.R. 6663, § 7(b)(2)(B), *with* S. 2261, § 7(c)(2)(B).

153. Sarbanes Report on H.R. 1, at 1. The For the People Act incorporates some of the provisions from earlier House and Senate election-security bills, but also reaches far more broadly.

154. "Requires states to use individual, durable, voter-verified paper ballots and that said ballots are counted by hand or an optical character recognition device." *Id.* at 5 (citing H.R. 1, 116th Cong. § 1502(a)(2)(A)).

state chief election officials from "participating in federal campaigns";[155] bars officials from using the power of their office to affect the results of elections;[156] regulates vendors of election systems by establishing cybersecurity and other standards;[157] creates a mechanism to provide grants to states for making upgrades to and maintenance of election systems, for adopting and using paper ballot systems, and for conducting post-election, risk-limiting audits;[158] and establishes an election systems vulnerability "bug bounty" program.[159]

In addition to the provisions seeking to protect the security and integrity of our electoral systems, the For the People Act also contains several provisions aimed at preventing corrupt conduct by federal public officials. These provisions do not directly, or even necessarily, involve election or voting systems. Nonetheless, we include some discussion of those provisions here for the lessons that they offer on possible anti-corruption measures, such as restrictions on lobbying activities and certain employment relationships within a specified period of entering or leaving government service, in the context of election security and integrity involving state and local election officials.

For example, the proposed bill would "[p]rohibit[] incentive payments from corporations to individuals entering government service."[160] It would also "[p]rohibit[] . . . procurement officers from accepting any compensation from a contractor to which the officer awarded a contract for two years after leaving government service."[161]

---

155. "Prohibits state chief election officials from participating in federal campaigns." *Id.* at 6 (citing H.R. 1, 116th Cong. § 1821).

156. "Prohibits using officials' authorities to affect the results of elections." *Id.*

157. "Establishes standards for election vendors based on cybersecurity and company ownership." *Id.* at 10 (citing H.R. 1, 116th Cong. § 298A).

158. "Allows the Election Assistance Commission to issue grants to states for improving and maintaining election systems[;] . . . for paper ballot systems[;] . . . [and] for risk-limiting audits after elections." *Id.* (citing H.R. 1, 116th Cong. § 1017). In contrast with the PAVE Act, however, the For the People Act would not make risk-limiting audits compulsory. Dell Cameron, *House Dems' First Bill Would Dramatically Boost Election Security*, GIZMODO (Jan. 4, 2019, 7:50 PM), https://gizmodo.com/house-dems-first-bill-would-dramatically-boost-election-1831504654.

159. "Establishes the 'Election Security Bug Bounty Program' to encourage independent assessments of election systems by technical experts." Sarbanes Report on H.R. 1, at 11 (citing H.R. 1, 116th Cong. § 3402).

160. *Id.* at 19 (citing H.R. 1, 116th Cong. § 202).

161. *Id.* (citing H.R. 1, 116th Cong. § 8004).

And it would "[p]rohibit[] a senior federal official from inappropriately using his or her position after leaving government service by restricting [him or her] from attempting to influence employees in the official's former agency for two years after the official's service ends."[162] Additional provisions would disallow congressional members from serving on the board of any for-profit entity,[163] and would "[c]odif[y] rules prohibiting [congressional] Members and staff from using official position to further their financial interests or the financial interests of their immediate families."[164]

We review the congressional activity recited above, not to take any position on the power or propriety of federal legislation in the areas coming within the scope of the proposed provisions, but rather to consider the kind of intervention state, county, and local authorities might use to address the problem of perceived illegitimacy of electoral outcomes caused by public officials' conflicts of interest and the appearance of conflicts of interest. The proposed federal legislation does not purport to directly address potential conflicts of interest by state public officials. In light of the threats to our democratic institutions posed by potential conflicts and the appearance of conflicts by election officials, we believe that state, county, and local governments should vigorously exercise their authority to ensure not only that the elections within their jurisdictions are trustworthy, but also that they are trusted.

Among the first priorities ripe for attention are updated, fully functional voting machines that use voter-verifiable paper ballots and produce an auditable paper record;[165] mandatory post-election risk-limiting audits;[166] and mandatory transparency and public-accountability procedures and reports.[167] These measures are urgently needed as a

162. *Id.* (citing H.R. 1, 116th Cong. § 8062).

163. *Id.* at 21 (citing H.R. 1, 116th Cong. § 9101).

164. *Id.* (citing H.R. 1, 116th Cong. § 9102).

165. Buchanan & Sulmeyer, *supra* note 18, at 14 ("A sizable percentage of precincts still use systems that are potentially open to manipulation and that sometimes also lack a voter-verifiable paper trail.").

166. Geller, *supra* note 42.

167. *See* Hill & Painter, *supra* note 7, at 1645 ("Transparency and accountability are the twin objectives of most regulatory schemes designed to uphold the fiduciary principle, whether in business organizations or in government.").

counterweight to increasingly intrusive cyber threats[168] and are consistent with cybersecurity and election experts' best-practices recommendations.[169]

Drawing upon some of the anti-corruption provisions in the For the People Act, public officials in state, county, and local governments can minimize the risk of conflicts of interest and the appearance thereof by adopting the following measures: (1) strict "anti-revolving-door" rules; (2) stringent, multiple-year disclosure requirements for campaign contributions and expenditures and other financial interests for all government officials, contractors, and sub-contractors who hold offices of public trust involving election and voting systems and processes; and (3) strict requirements that public officials recuse themselves from any oversight, administration, auditing, or certifying of any elections in which the official or his or her immediate family member is a candidate.[170]

Some jurisdictions have begun acting on the first set of recommendations. For example, in recognition of the need for public confidence in voting tallies, the City of Fairfax, Virginia, and Orange County, California, administered a pilot program in the 2018 midterm elections using risk-limiting audits based on a paper-record voting trail.[171] Similarly, and for the same reason, the State of Colorado has adopted paper ballots and risk-limiting audits statewide.[172] But obviously much work remains to be done if the existing vulnerabilities in the nation's electoral systems are to be protected.

---

168. "In the last two years reports of unprecedented cyber threats against U.S. election infrastructure have blanketed the news and rattled public confidence." *See* Geller, *supra* note 48; *see also supra* text accompanying note 48.

169. *See supra* Section IV.B.

170. *See supra* text accompanying notes 153–64.

171. "A voting system that produces accurate results, but provides no way to know whether it did, is inadequate. It provides far too many ways for resourceful adversaries to undermine public confidence in election integrity." MARK LINDEMANN, *supra* note 46, at 4–5 (noting that "evidence-based" elections such as risk-limiting audits meet the requisite elements for ensuring accurate vote tallies and promoting voter confidence in election integrity: "use paper ballots, protect them, and check them"); *see also* Vasilogambros, *supra* note 34 ("'Audits empower people to feel like their vote counted and feel engaged in the process,' said Aquene Freechild, co-director of nonprofit Public Citizen's Democracy Is For People campaign. 'Voters in states and counties that lack audits cannot be sure their votes were fully counted,' she said.").

172. Geller, *supra* note 42.

VI. CONCLUSION

The cold-as-steel insight captured in Stalin's infamous dictum is that elections are, most importantly, about the acquisition of power; and that by this measure it is not the casting but the counting of ballots that matters. Lest the American electorate succumb to a similar cynicism, as Stalin's successor in interest ardently seeks, our public officials must scrupulously guard voting procedures from the risks of electronic tampering, both by adopting best practices *ex ante* and by conducting thorough audits where appropriate *ex post*. Ultimately, nothing less may once again be at stake than whether government "of the people, by the people, for the people shall not perish from the earth."[173]

173. Abraham Lincoln, Gettysburg Address (Nov. 19, 1863).