Election Security & the Right to Vote

Rights and Remedies Implicated by Election Hacking

NOVEMBER 2018

Protect Democracy

Altshuler Berzon LLP

EXECUTIVE SUMMARY

Should our nation be confronted on or after Election Day with credible evidence of a hack impacting an election, there will be a need for clear-headed action—under extreme time pressure—to protect the integrity of our democracy and the fundamental right to vote. This paper provides an overview of some of the key legal issues that would be relevant to lawyers or courts facing such a scenario. Its aim is to provide guidance so that litigants and courts can find practical ways to remedy the effects of a hack in a way that is consistent with applicable legal requirements and reflects the importance of accurately counting every single ballot.

Part I discusses the legal framework governing elections and the right to vote. We discuss how the Equal Protection Clause, Due Process Clause, and other federal constitutional protections would be implicated by a breach of electronic voting systems. In particular, we explain that the U.S. Constitution imposes a duty on state and local officials to protect the right of qualified voters to cast their votes *effectively*, and prohibits states and local jurisdictions from operating unacceptably vulnerable elections systems that result in a breach that alters votes or prevents the ability to vote. We also discuss federal statutory protections as well as state constitutional and statutory frameworks that could be implicated by a breach of these systems.

Part II discusses potential remedies that may be available in post-election legal challenge arising from evidence that hacking may have affected election systems and outcomes. We discuss recounts, audits, delays in certification of a final vote count, injunctions preventing a candidate from taking office, orders adjusting or reforming the vote count, orders to re-run an election or conduct a special election, and orders pertaining to future elections. Though the availability of any potential remedy would be highly fact-specific and depend on the particular forum in which litigation occurs, we outline the key considerations for litigants and courts.

Part III discusses some additional considerations that may be relevant in a post-election legal challenge based on evidence of a cyber-security breach. We discuss potential plaintiffs and standing issues, potential defendants, and evidentiary and discovery considerations, including likely sources of relevant information, as well as timing and confidentiality considerations.

Throughout, we focus the discussion on five hypothetical fact scenarios: (1) hacking that implicates the recording of votes; (2) hacking that impacts vote tallies; (3) hacking of voter registration records; (4) ballot alteration; and (5) hacking that results in election-day chaos and interference with voting. We do not provide an exhaustive discussion of each of these scenarios or a roadmap for pursing or defending any particular claim or achieving any particular remedy. Rather, we use these scenarios to provide a structure for those seeking to find effective and legally appropriate responses to the possible cyberattack of an election.

We hope that the scenarios discussed in this paper remain hypothetical. But should they not be, this paper is intended to assist those seeking to protect the integrity of the democratic enterprise by providing an orderly framework for navigating the complex issues raised in the chaotic, fast-paced post-election context.

TABLE OF CONTENTS

INTRODUCTION

Ensuring the security of our nation's electronic voting systems is critical to maintaining the integrity of our democracy and protecting the right to vote. In recent years, national security and cyber-security experts have made clear that some of our nation's electronic voting systems, particularly those relying on older technology, may contain security weaknesses susceptible to being breached.[1] And, as the evidence of interference by foreign interests in the 2016 election and the intelligence community's warnings of 2018 interference efforts make plain, the risk is no longer theoretical.[2] With the assistance of the federal and state governments, many local jurisdictions have worked diligently to replace older technology and to secure systems against these risks—but as with all aspects of our federalist election system, that work has been inconsistent across jurisdictions.[3] If electronic voting systems with security flaws are exploited before or during the 2018 election, impacted voters, candidates, and courts will need to navigate a complex web of law very quickly. This paper provides a high-level overview of the many legal issues raised in the post-election context should state or local voting technology, software, data, or networks be subject to a breach on or before Election Day.

Security breaches and hacks of electronic voting systems and voter registration systems used by states and localities to conduct elections implicate the right to cast a ballot and have it accurately counted—a right protected by the U.S. Constitution. The U.S. Supreme Court has long recognized that the right to vote is fundamental and "preservative of all rights."[4] Any analysis of the legal implications of the impacts of election hacking on the right to vote cannot, however, begin and end with the federal Constitution. The administration and conduct of elections and the right to vote at the federal, state, and local levels involve a complex system of federal and state constitutional and statutory law, and in some places local ordinances.

This paper focuses not on pre-election actions challenging paperless or outdated voting systems, but on a hypothetical post-election context in which there is credible evidence that a hack has impacted the administration or outcome of the election. We outline the types of rights implicated by the various impacts hacking could have on an election, the potential remedies available in state and federal courts to ensure that votes are properly cast and counted, and other litigation considerations. This paper is not intended to be exhaustive with respect to these topics, or to provide a roadmap to pursuing or defending any particular claim. Instead, we have identified issues that would have to be carefully examined and analyzed in the event of a cyberattack, taking into account the scope of the problem, the history of officials' efforts to address election security gaps, and the laws of the relevant jurisdictions.

To frame this discussion, we focus on the following hypothetical scenarios:

1. *Hacking that impacts the recording of votes.* In some jurisdictions, electronic voting machines and vote tabulation software may be vulnerable to hacking that could impact the recording of votes. Fourteen states use machines that lack any paper trail of votes cast, meaning that the only record of votes cast is a digital one.[5] In some cases, machines may be connected (or connectable) to networks that are susceptible to hacking. A breach of this nature could vary in scope, ranging from impacting machines in multiple states to those in just a single precinct.

2. *Hacking that impacts vote tallies.* Systems and networks used to record official vote tallies may also be susceptible to breach at the precinct, county, or state level. The lack of a paper trail in some jurisdictions would impact the severity of this problem.

3. *Hacking of voter registration records.* The systems and networks that store voter registration records are often online, and thus—to varying degrees depending on a jurisdiction's precautions—susceptible to breach.[6] If a voter's registration is deleted or significantly altered, that voter may not be permitted to cast an in-person ballot, be required to vote a provisional ballot, and have that provisional ballot rejected without recourse.

4. *Ballot alteration*. The electronic systems on which official ballots are created and stored could be breached to cause the deletion or addition of candidates or entire races, or to otherwise alter ballots to create confusion or votes that do not reflect voter intent.

5. *Hacking that results in election-day chaos and interference with voting*. System or machine malfunction could cause widespread disruption of voting, leading to long lines, voter confusion, and voters being prevented from voting—particularly if election officials are unprepared for this contingency and lack sufficient paper ballot alternatives.

LEGAL ANALYSIS

I. Legal Framework Governing Elections and the Right to Vote

The authority and responsibility to conduct elections, including elections for federal office, is delegated by the U.S. Constitution to the states.[7] The Constitution also constrains the latitude granted to the states in conducting elections by imposing on those states a duty to protect the right to vote. This fundamental right, and the states' duty to protect that right, is reflected in several constitutional provisions, including: the Due Process and Equal Protection Clauses of the Fourteenth Amendment; the First Amendment; the requirement in Article I, Section 2 and the Seventeenth Amendment that Congress be elected by "the people;" and in the protections in the Fifteenth, Nineteenth, and Twenty-Sixth Amendments from infringement by the government of the right to vote on the basis of race, sex, and age.[8]

At the federal level, Congress has also exercised its authority to regulate the states' conduct of federal elections and to implement protections for constitutional rights through, for example, statutes governing the administration of federal elections (the Help America Vote Act), voter registration (the National Voter Registration Act), and prohibitions on discriminatory voting practices (the Voting Rights Act).[9] States have corresponding laws that both create the complex apparatus for the administration of elections at the state and local levels and impose protections for the right to vote.[10] These include civil and criminal statutes and state constitutional provisions, some of which provide greater protections for the right to vote against infringement by government officials than federal law.[11]

A. Federal Constitutional Protections

The U.S. Constitution protects not just the right to cast a ballot, but to have that ballot counted: "the right of qualified voters . . . to cast their votes *effectively* . . . rank[s] among our most precious freedoms."[12] As the complexity of election administration at the state and local level has grown, the Supreme Court has increasingly recognized that the Constitution protects "the right to participate in an electoral process that is necessarily structured to maintain the integrity of the democratic system."[13] The constitutional protection for the right to vote generally takes three forms: 1) protection against laws, regulations, or official actions that deny or unduly burden the right to vote; 2) protection against voting systems that are fundamentally unfair; and 3) protection against laws, regulations, or official actions that treat voters unequally with respect to the franchise. Reflecting the multiple constitutional sources protecting this fundamental right, these theories are not mutually exclusive, and governmental action that infringes the right to vote may violate the constitution in more than one manner. Congress has established a federal cause of action pursuant to 42 U.S.C. § 1983 for the violation of federally-protected constitutional rights by state actors, including the right to vote.

1. Unlawful Denial of or Burdens on the Right to Effectively Vote

States and localities may not, consistent with the constitutional protections for the right to vote, deny or burden otherwise qualified voters' right to vote, without furthering a sufficiently legitimate, specific, and weighty state interest.[14] Courts evaluating constitutional claims implicating the right to vote must weigh "the character and magnitude of the asserted injury" against "the precise interests put forward by the State as justifications for the burden imposed by its rule, taking into consideration the extent to which those interests make it necessary to burden the plaintiff's rights."[15]

Courts use this balancing test to determine the level of scrutiny to apply to governmental action that implicates the right to vote: state laws or conduct that impose a "severe" burden on the right to vote are unconstitutional unless justified by "a narrowly drawn state interest of compelling importance."[16] But "[h]owever slight [the] burden" on the right to vote "may appear, . . . it must be justified by relevant and legitimate state interests 'sufficiently weighty to justify the limitation.'"[17] In assessing whether to impose strict or lesser scrutiny, courts consider whether the disqualification of ballots (or other burden on the right to vote) is wholly unrelated to voter qualifications or voter error.[18] In assessing whether a state law imposes "severe" rather than "reasonable" restrictions, the Supreme Court has also focused on whether alternative action is available to voters to ensure their votes count.[19] This analysis involves not bright-line rules, but a fact-intensive inquiry.[20]

These principles have guided lower courts in assessing challenges to unreliable election systems that threaten to deny the right to vote to otherwise qualified electors.[21] Applying these legal standards to the impact on the administration of an election under the various hacking scenarios would require careful analysis of the facts and law of the affected jurisdiction.[22] Some key considerations would include:

a. *Hacking that impacts the recording of votes.* Where the exploitation of a cyber-security weakness in electronic voting machines results, or appears to result, in inaccurate vote counts, otherwise qualified voters would be actually disenfranchised through no fault of their own. Courts should therefore apply strict scrutiny in this scenario to determine whether the actions of state or local officials responsible for the voting system violated the constitutional protection for the right to vote.[23] The constitutional question will focus on whether the actions by government officials in conducting the election, including the choice and administration of any technology and security measures used, were narrowly tailored to achieving a compelling state interest.

Because the justifications for using certain election systems will vary by jurisdiction, careful attention must be paid to the factual history of the machines, software, networks, and other technology implicated by the hack; the history of complaints or knowledge of security flaws; and the action (or inaction) of local or state officials in addressing these issues; and the availability of more secure alternatives. Lack of a paper vote trail will be significant as a factual matter and as a legal matter, both because the widespread availability of more verifiable and less vulnerable systems means a choice to use less secure machines may not pass strict scrutiny, and because the lack of a paper trail will affect potential remedies.

b. *Hacking that impacts vote tallies.* The alteration of vote tallies resulting from the breach of an insecure system may likewise be subject to strict scrutiny: votes of otherwise qualified voters, through no fault of their own, have been changed, deleted, or diluted. Again, the question would be whether the maintenance and use of an insufficiently secure election system was narrowly tailored to achieving a compelling state interest.

c. *Hacking of voter registration records*. In some jurisdictions, voter registration databases are in fact susceptible to hacking, and therefore to alteration.[24] A hack where records are altered to eliminate voter registrations would effectively purge the voter rolls without notice to affected voters. Voters would attempt to vote, be missing from the rolls, and therefore be forced to cast a provisional ballot. That ballot would eventually be rejected for lack of matching registration. This would result in direct disenfranchisement of voters, through no fault of their own, for reasons unrelated to their actual qualification to vote. To satisfy strict scrutiny, a jurisdiction would be required to justify the use of a fundamentally insecure system for maintaining voter records.

Voter registration records could also be subject to more subtle changes than deletion. For example, in jurisdictions where voter identification is required to match voter registration, a hack that merely altered voter names or addresses in the voter registration database could result in total disenfranchisement of the affected voters—again unrelated to actual voter qualifications and with no reasonable opportunity to cure. There are cases involving sporadic or infrequent errors in voter records that might not amount to a constitutional violation, so the success of a claim here may turn on whether the hack resulted in errors past a certain error rate threshold.

d. *Ballot alteration.* If a hacker exploits a security weakness to remove a candidate entirely from the ballot, the right to cast an *effective* ballot is implicated. Very generally speaking, the addition of candidates to a ballot or other inaccuracy in the candidate names that would arguably dilute the vote will have to overcome precedent permitting, under certain circumstances, disqualified candidates to remain on ballot and other ballot flaws.[25]

e. *Hacking that results in election-day chaos and interference with voting.* Litigation claiming that exploitation of security weaknesses in the electronic elements of a voting system led to long lines, increased time periods, or difficulty voting would also be analyzed under the *Burdick* sliding scale to determine whether the problem constitutes a severe burden on the right to vote or merely the sort of administrative burden that affects any election. The extent of the burden is, of course, only one half of the equation, and assessing the state interest would depend on the specific elements of a state's system being challenged in litigation as unduly vulnerable.

2. Fundamentally Unfair Voting Systems

The Due Process Clause of the Fourteenth Amendment also protects against voting restrictions that render a voting system "fundamentally unfair."[26] While "garden variety election irregularities" do not rise to that level, state election procedures and standards run afoul of due process if they "result in significant disenfranchisement and vote dilution."[27] Courts have consistently held that once state actors have induced a voter's reliance on a particular manner of voting, invalidation of that voter's ballot is "fundamentally unfair."[28] Courts thus attempt to police the line between "sporadic" or "episodic" errors in a voting system (held to be "garden-variety" and therefore not a violation), and pervasive problems that permeate a voting system (or result in a substantial rate of error or risk of error) that rise to the level of a federal constitutional problem.[29] Courts have also examined whether state procedures provide for adequate corrective measures to address the problem.[30] Some federal courts have expressed a desire to avoid micro-managing election recounts that are also being managed by state courts, even where errors may be outcome determinative.[31] As with many federal constitutional questions in the realm of voting, there is no bright-line rule.

A hack targeting insufficiently secure voting machines, voter rolls, or tabulation devices might cause an election to be conducted in a fundamentally unfair manner if it: (a) led to excessive lines at polling places, requiring voters to wait for hours to cast a ballot;[32] (b) caused the loss of a significant percentage of ballots cast or appeared to "flip" a significant number of votes;[33] (c) prevented the counting of significant numbers of ballots cast by qualified voters;[34] or (d) prevented voters from casting a ballot due to malfunctioning or non-functioning machinery.[35] The facts—in particular the scope of the problem created by hacking and the actions of the public officials in charge of the election before and after the hack—will make a great deal of difference.

3. Equal Protection Against Variation within a Jurisdiction

The Equal Protection Clause of the Fourteenth Amendment also protects voters from government action that results in unjustified disparities between voters (or categories of voters) within a jurisdiction. "Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another."[36] Thus, the Equal Protection Clause is implicated not only when some individuals face a disproportionate burden in accessing the ballot, but when some voters' ballots are less likely to be counted than others.

Where categorical distinctions between voters exist on the face of a law or procedure, the analysis is relatively straightforward.[37] However, election administration in the United States involves a great deal of variation, including within jurisdictions. *Bush v. Gore* recognized that an equal protection claim may be based not only on categorical distinctions, but also on arbitrary disparities in the treatment of voters.[38] But, *Bush v. Gore* but provided little guidance to lower courts regarding when such variation becomes a constitutional concern, and this remains a gray area.

Each of the hacking scenarios could, depending on the facts, reflect conduct by governmental officials—in using and administering election systems susceptible to breach and that were actually breached—that can result in arbitrary disparities among voters within or between jurisdictions:

a. *Hacking that impacts the recording of votes.* The use of different types of voting machines by and within jurisdictions may raise this type of equal protection concern, should the more flawed systems be breached and not the others. "[T]he lack of statewide standards [may] effectively den[y] voters the fundamental right to vote."[39]

Even where there is no variation in the types of voting machines involved, the exploitation of security weaknesses in electronic voting systems that deleted or altered some but not all of individual voters' ballots within a jurisdiction would necessarily result in the disparate and arbitrary treatment of votes, raising equal protection concerns. Likewise, if hackers were able to exploit a security weakness to target the votes of a group of individuals by which party or candidate they were voting for, or by some personal characteristic such as, for example, voters in primarily African-American precincts, the conduct and certification of the results of such an election could raise equal protection concerns.

b. *Record system hacking that impacts vote tallies.* The improper alteration of particular vote tallies would disparately impact the right of certain voters to have their votes effectively counted. In addition to implicating the fundamental fairness of the entire system, altering the election outcome (presumably to flip votes or add or subtract votes for particular candidates) would necessarily also implicate equal protection concerns arising from arbitrary disparities that are no fault of the voter.

c. *Hacking of voter registration.* Unless *all* voter registration records within a jurisdiction are altered as a result of a cyber-security breach, the deletion or alteration of some voters registration records likewise implicates the arbitrary, disparate treatment of the affected voters.

d. *Ballot alteration and hacking that results in election-day chaos and interference with voting.* These are fact-specific scenarios that, if they impact some voters and not others within a jurisdiction, will implicate equal protection concerns.[40]

B. Federal Statutory Protections

Two federal statutes governing election administration could be implicated by the effects of hacking on election administration: the National Voter Registration Act ("NVRA" or "motor voter law"), 52 U.S.C. § 20501 *et seq*.; and the Help America Vote Act ("HAVA"), 52 U.S.C. § 20901 *et seq*.

The NVRA establishes certain voter registration requirements with respect to elections for federal office and specifically prevents voters from being removed from the rolls except in narrow circumstances.[41] Any breach of electronic systems that results in otherwise qualified voters being removed from a state's voter registration records arguably results in a violation of this provision—importantly, the statute is not limited to removal by the state, but prohibits any removal inconsistent with the statute.[42] The NVRA provides a private right of action to any "aggrieved" person.[43] This provision against removal is also enforceable through HAVA.[44]

Title III of HAVA also imposes specific provisions pertaining to the security of electronic voter registration records, and minimum standards, including error rates, for electronic voting equipment.[45] While states are bound to comply, the courts that have considered the question have either concluded that HAVA does not create a private right of action to enforce these provisions, or have avoided resolving that issue while suggesting that a private right of action is probably not available.[46]

C. State Law

1. State Constitutions

All states but Arizona explicitly grant the right to vote in their constitution.[47] Twenty-six states have constitutional provisions guaranteeing that elections be "free," "free and equal," or "free and open."[48] Some state courts have interpreted this language to establish a *broader* right to vote than that articulated by the federal courts and, accordingly, have rejected U.S. Supreme Court voting rights cases as binding precedent in favor of greater protections for the "fundamental right to vote."[49]

State courts have construed this language—"free," "free and equal," or "free and open"—to require a new election where errors on the ballot or with ballot counting may have affected the results. For example, Kentucky courts, which have "the most developed jurisprudence of any state on what [the 'free and equal'] clause means in relation to ballot problems,"[50] have held that "no election can be free and equal . . . if any substantial number of persons entitled to vote are denied the right to do so."[51] The Kentucky Supreme Court has invalidated election results where ballots failed to list the proper candidates in a subset of precincts,[52] where ballots listed the wrong candidates in one precinct of three,[53] and where the county clerk omitted the name of one qualified candidate from all ballots.[54]

But other state courts have interpreted the express constitutional guarantee of "free and equal" elections to be not more than co-extensive with the federal constitutional right to vote.[55] These courts generally apply the *Burdick* framework to state constitutional challenges alleging infringement of the right to vote.

2. State Statutes and Common Law

Canvassing the myriad state election law requirements implicated by the effects of various hacking scenarios, including the rights and remedies available in state election challenge procedures, is beyond the scope of this paper. As a brief overview of issues raised by state law election challenges:

a. *Who may bring a challenge?* State law varies with respect to whether voters, candidates, or either may challenge election results.[56]

b. *Who may hear a challenge?* Most states direct election contest proceedings to state courts. A few states grant primary or exclusive jurisdiction to state legislative bodies or elected officials, rather than the courts.[57]

c. *What races may be challenged?* Some states permit election contests to the outcome of any race (local, state, or federal).[58] Other states decline to grant jurisdiction to any state body for challenges to the outcome of elections for federal office.[59]

d. *On what grounds can elections be challenged?* Broadly speaking, state statutes provide relief under two circumstances: (1) where the result has been called into question because illegal votes were cast or legal votes left uncounted, or (2) where officials have engaged in fraud, misconduct, or other irregularities.[60]

States frame the substantive protections of these laws in different ways. Louisiana's statute, for example, focuses on the effect on the outcome of the election.[61] Courts have construed this statute, however, to cover circumstances in which "the proven frauds or irregularities are of such a serious nature so as to deprive the voters of the free expression of their will," even if the number of affected ballots is unclear.[62] Ultimately, it is "the effect of irregularity on determining the outcome . . . that must be considered."[63]

Texas, similarly, will consider challenges addressing "whether the outcome of the contested election, as shown by the final canvass, is not the true outcome because (1) illegal votes were counted or (2) an election officer or other person officially involved in the administration of the election: (A) prevented eligible voters from voting; (B) failed to count legal votes; or (C) engaged in other fraud or illegal conduct or made a mistake."[64]

Florida law, in contrast, focuses on procedural errors, and requires only "reasonable doubt" as to the accuracy of the supposed outcome: "An election should not be set aside unless a court finds substantial non-compliance with a statutory election procedure and also makes a factual determination that reasonable doubt exists as to whether a certified election expressed the will of the voters."[65]

II. Potential Remedies for Post-Election Claims Arising from Effects of Hacking on Election Systems and Outcomes

This section addresses remedies that may be available in post-election legal challenges arising from evidence of hacking or a risk that an election has been hacked. Of course, state and local officials may act to remedy the impacts of a security breach without any need to resort to administrative action or litigation. And, there is no one-size-fits-all remedy: the nature and scope of the alleged hack, and the jurisdiction involved, will impact the range of procedures and remedies available if a challenge were ever warranted.

State and local laws generally provide methods for reviewing and contesting election outcomes (including for federal, state, and local office), including recount and audit measures and election contest procedures. These procedures are part of routine election administration, and most states have highly detailed statutory provisions setting forth the steps for either automatically triggering a recount or permitting individuals to request a recount of the ballots—typically including contest provisions for elections that are not resolved by an automatic recount or recount on demand.[66] As a broad generalization, because state recount and audit procedures were not written to accommodate and deal with the myriad concerns that arise from a hack, a recount of a hacked vote may result in an identical count that is just as compromised by the hack as the original vote count. This is particularly true for paperless electronic voting systems.

Equitable remedies for federal constitutional and statutory violations may also be available in federal court. Post-election remedies challenging the outcome of the election generally face a high bar and will require showing some relationship between the alleged violation and the outcome of the election (ranging from substantial impact to proof that the violation was outcome determinative, depending on the nature of the violation).[67] Moreover, the availability and scope of state court contest remedies may impact whether certain equitable remedies are available directly in federal court for federal constitutional violations.[68]

Importantly, the time frame for recount procedures available under state and local law is generally very fast, and review is often limited to a specified universe of materials (the paper trail, the voting record, the actual ballots, the county's voter registration records, etc.).[69] Timing considerations include: the relevant state and federal deadlines for counting and certification of the offices at issue; the length of time for any forensic analysis of affected machines or investigation of the hack; time needed to address disputes arising from vendor interest in maintaining the confidentiality of "trade secrets" pertaining to election equipment; and the length of time needed to access the voting data and conduct a statistical analysis. State law deadlines may give way to federal constitutional concerns, and federal constitutional deadlines may need to be reconciled with other federal constitutional protections. Exacting analysis of all of the deadlines relevant to the particular violations will be necessary, as none of the deadlines at issue will be long.

Given the unforgiving timeline, it is likely that litigants may file parallel actions, including state law administrative processes, state court litigation, and federal court litigation addressing both the state challenge process itself and more substantive arguments around the effect of the alleged hack.[70] A key challenge for all parties in this circumstance will be ensuring efforts are properly coordinated—particularly where parallel actions involve interlocking issues.

Below, we identify a range of possible post-election remedies that may be available to address the types of hacking scenarios previously identified.

A. Recounts and Audits

States have widely varying statutory requirements for recounts or audits of vote tallies.[71] Most states mandate recounts when the margin of victory is within a specified range, and many also have provisions that permit recounts upon request of a candidate or voter (usually at their expense). Recounts may have multiple stages, including an initial re-review of votes counted and votes rejected.[72] Difficulties arise where states use direct-recording electronic voting ("DRE") machines, particularly those without a paper record.[73] It is unlikely that the various state law recount procedures provide a systematic remedy that can address the widespread hacking of voting machines, vote tallies, or voter registration records; ballot alteration; or election day chaos.

State audit procedures are likewise unlikely to provide a substantial remedy for problems caused by hacking, although they may help identify a problem. Some states—like Georgia—do not require any audits following an election. Other states have rigorous audit requirements.[74] However, in many states, audits are generally conducted only *after* an election is certified, and are not self-executing as to any errors uncovered.[75] Finally, in some states the audit statute does trigger a recount where the hand- and machine-tabulated vote differ.[76]

While recount and audit procedures may be a place to start in examining the election results in the context of hacking concerns, they are ultimately of limited usefulness. Moreover, from the voter's perspective, they can often be quite costly and difficult. And, as a practical matter, in paperless systems recounts may simply confirm the hacked votes with no verifiable way to determine actual voter intent. Where the vote tally has been altered, recounts may not even be available where the resulting margin of victory is intentionally large enough to avoid state recount provisions.

Whether a court-ordered recount or review of all or some of the ballots cast or rejected is an appropriate or available remedy, in addition to any state-mandated recount procedures, will depend on the nature and scope of the problem identified and a careful analysis of the law of the jurisdiction.[77]

B. Delaying Certification of Final Election Results and/or Injunction Preventing Candidate from Taking Office

Because states generally have short statutory deadlines for certification of the final vote counts and the seating of election winners, court orders extending those deadlines might be sought to allow for sufficient time to conduct necessary discovery and resolve disputes related to election hacking.[78] For example, a Louisiana state trial court issued a temporary restraining order prohibiting certification of vote totals until an evidentiary hearing could be held to address voting machine error.[79] A trial court in Arkansas issued a similar temporary restraining order, barring the apparently winning candidate from being sworn in until an evidentiary hearing could be conducted in the apparent losing candidate's election contest litigation.[80]

When presented with evidence of constitutional violations affecting the outcome of a vote, federal courts may also issue preliminary orders delaying certification of a final vote count and preventing an apparent winning candidate from taking office.[81] For example, in *Shannon v. Jacobowitz*, 301 F. Supp. 2d 249, 251 (N.D.N.Y. 2003), a federal district court in New York issued a temporary restraining order, and subsequently a preliminary injunction, enjoining a county Board of Elections from certifying the winner of a disputed town supervisor election and enjoining the apparent winner from taking office, where the plaintiffs presented undisputed evidence that the opposing candidate was wrongfully denied at least 69 votes because of a voting machine malfunction.[82]

Other procedural options might also be available to quickly address uncertainty in the context of a post-election challenge based on evidence of hacking. A federal court has the authority, for example, to appoint a special master with technical expertise to address technical factual issues under Federal Rule of Civil Procedure 53, although the circumstances when such an appointment would be helpful within the extreme time constraints of post-election proceedings may be limited.

C. Order Requiring Examination of Voting System Hardware and Software

In the case of any hack or suspected hack that impacts an election, court-supervised review of actual ballots or their electronic equivalent, or even a full-blown evidentiary hearing, may be needed to determine whether election results have been distorted. State courts have occasionally engaged in direct fact-finding as to the validity of ballots. Although the forensic examination of electronic voting equipment presents technical complications beyond a facial review of the markings on a paper ballot, in other contexts trial courts have resolved contested questions of whether a ballot as counted reflects a voter's intention. For example, in *Womack v. Foster*, 8 S.W.3d 854 (Ark. 2000), the trial court determined after an 11-day trial that 518 absentee ballots for the putative winner were invalid and ordered the opposing candidate—who after the invalid ballots were struck had the higher total—the winner.[83] Likewise, the federal court in *Hunter* swiftly ordered the county board to investigate the accusations of poll-worker error resulting in invalid provisional ballots during the state law recount process.[84]

D. Order Reforming the Vote Count

When election officials have improperly excluded ballots from vote totals, courts have ordered improperly excluded ballots opened and counted, and thereby adjusted vote totals.[85] If a hacking scenario involves *deleting* otherwise valid votes for a particular candidate, assuming difficult questions of factual proof can be resolved, the remedy of adding those votes back in and reforming the vote total should be possible. This likewise should be a possible remedy (again, assuming difficult questions of proof are resolved) for any provisional ballots that are cast but not counted because voter registration records have been deleted: because those ballots would have been segregated and are identifiable by name, a court could identify the properly registered voters and order their ballots opened and counted. The scope of the hack and the availability or absence of a paper trail will affect the efficacy of these remedies.

More difficult remedial questions are raised by some of the other hacking scenarios, where in-person votes are not recorded and therefore not counted, or where improper votes are *added* to the vote count. When confronted with conclusive evidence of ballots improperly included within a vote total, some courts have chosen to invalidate a subset of the ballots cast rather than leaving the vote count intact or nullifying the election in its entirety.[86] When the concern is with respect to absentee or provisional ballots, the ballots are likely to have been segregated, making it possible to accurately revise vote totals. For example, in a case involving potentially altered paper ballots, the Pennsylvania Supreme Court ordered a trial court to individually review ballots determined to have been altered between the initial vote tally and the recount and invite affected voters to testify as to who they voted for, in order to determine the true election results.[87] However, this invalidation-and-reformation remedy may not work as well where the issue concerns vote totals from in-person voting: the improper ballots could have been physically mixed with valid ballots or, in the case of DRE machines, simply included in the digitally-recorded totals. Courts in at least two states where it was impossible to segregate the affected ballots (and therefore identify the votes cast), have ordered *all* absentee ballots, or all ballots cast in a particular precinct, invalidated—including legal ballots.[88] Any order removing invalid *and* valid ballots from the vote total and ordering a new election result certified raises concerns about the rights of the voters who cast valid ballots.

Other remedies short of requiring a re-run election—including the possibility of "proportional deduction" or resort to a statutory tie-breaker method—might also be worth consideration in certain circumstances.[89]

E. Re-running the Election or Running a Special Election

Although rare, some courts have ordered special elections as a remedy for election errors. Indeed, some states have specific statutes providing for special elections in certain circumstances.[90] Relying on such a statute, the Indiana Supreme Court ordered a new Democratic Party primary for mayor of the City of East Chicago where problems involving absentee ballots "so infected the election process as to profoundly undermine the integrity of the election and trustworthiness of its outcome."[91] Other state courts have ordered new elections when faced with evidence that the outcome of an election was suspect, particularly where so many votes were invalid that it was impossible to determine the will of the voters, or where the evidence suggested a widespread problem of unknown scope. The Mississippi Supreme Court has ordered new elections where evidence established that a relatively small number of ballots were not properly counted, supporting an inference that the problem was actually widespread.[92] State courts apply widely varying substantive standards for determining whether to order a re-run election in the context of state election contests, and some states require a different showing depending on the type of challenge.[93]

The barrier to a federal court ordering a re-run election is high: although federal courts that have addressed the issue have not settled on a consistent standard, all agree that the burden on challengers is heavy, and that new elections are appropriate only where the integrity of the election mechanism, and not just the result, has been called into doubt.[94]

Any security breach that results in the alteration of a large number of votes—either by altering vote tallies for specific candidates, deleting vote tallies altogether, or eliminating candidates from ballots cast by a significant number of voters—would be analogous to problems that have, on occasion, resulted in courts ordering new elections. Whether such a remedy is warranted or authorized will require close analysis of the applicable facts and law of the relevant jurisdiction.

Importantly, in the context of alleged cyber-security failings, there is an additional, critical concern. Re-running an election on the same insecure or compromised machines, software, and network, with the same security flaws, would be an inadequate remedy. Any request for a special election would require quickly identifying feasible security measures to address the problems that resulted in the election errors or cyber-vulnerability in the first election.

F. Orders Pertaining to Future Elections

While any court will focus its attention and resources on whether to grant emergency remedies in the immediate aftermath of an election, evidence of hacking could also be strong evidence that a jurisdiction's procedures or equipment should be fixed going forward. State court election contests may not permit the courts to consider the question of permanent injunctive relief that goes beyond the election in question; further relief at the state level would therefore require filing a separate lawsuit seeking a permanent injunction. But any federal case challenging constitutional violations could, and likely should, address the question of forward-looking relief as the case proceeds.

III. Litigation Considerations

Litigation is, of course, not the only means of resolving concerns regarding the impact of a hack on an election. First and foremost, the elections officials running the election have a duty and obligation to investigate and remedy what they can, within the bounds of their authority under local and state law. These officials, including the state's chief elections officer, bear responsibility for ensuring the accuracy of voting records and vote counts. They may identify the problem and propose solutions in the immediate aftermath of an election—but, depending on state law and the boundaries of their authority, officials may feel constrained in the possible remedies they can offer. Where election officials have not adequately addressed problems caused by a hack, litigation may provide an option for enforcing rights and remedies available to impacted voters, candidates, and organizations. We focus here on considerations that would apply to affirmative litigation brought by those seeking to protect the right to vote.

A. Potential Plaintiffs and Standing

To bring a federal constitutional or statutory challenge to an election impacted by hacking, a plaintiff must demonstrate that he or she meets the constitutional requirements of standing. To establish standing, a plaintiff must have "suffered an injury in fact—an invasion of a legally protected interest that is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of. . . . Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."[95]

1. Injured Voters, Organizations, and Candidates

The U.S. Supreme Court has recognized that "where large numbers of voters suffer interference with voting rights conferred by law," the injury—although widely shared—is concrete and specific enough to support standing.[96] Individual voters who can demonstrate that their ballots or voter registration records were actually misallocated or destroyed as a result of a hack would have an injury in fact sufficient for Article III standing purposes. However, a voter need not show that his or her ballot was actually destroyed or altered as a result of a security breach. Courts have found standing where voters showed a significant possibility that their own ballots were or are very likely to be affected.[97] The probability that one's vote will be improperly discounted should be enough to confer standing.

In a jurisdiction where evidence points to a hack impacting votes or vote tallies, voters can also establish injury by showing dilution of their vote (as in the case of deleted votes, added votes, or flipped votes).[98] In the case of election hacking that causes widespread malfunctions leading to difficulty voting, including long lines, malfunctioning voting equipment, or a lack of paper materials for back-up voting, voters impacted by those problems can assert standing as well.[99]

Finally, for equal protection claims where some, but not all, precincts or machines were affected by an attack, voters within the affected group would have standing. But a voter might also have standing if a hack caused a vote tabulation to be artificially inflated, even if his vote was cast outside the affected precinct, because his properly counted vote was diluted by the incorrect vote count.

Voting cases may be, but need not necessarily be, brought on behalf of a plaintiff class of affected (or potentially affected) voters.[100] The question of whether a class action is appropriate, and whether class certification requirements are satisfied, may turn on the scope of the problem (confined to one county, multiple counties, and entire state), and the nature of the injunctive relief sought. Certain organizations may have standing to bring claims using associational[101] and organizational[102] standing. And where a political candidate alleges that the impact of the breach has made the will of the voters impossible to discern or has altered the vote count such that the unsuccessful candidate in fact received more legitimate votes, that candidate may have standing to bring a constitutional challenge to the election results. Courts are not generally opposed to adjudicating the rights of voters in a suit brought by a candidate.[103] Accordingly, federal courts, including the U.S. Supreme Court, have issued opinions on candidates' constitutional challenges to election procedures without discussing *why* the candidate had standing to bring claims of constitutional violations committed against voters.[104]

2. Causation and Redressability

Any lawsuit brought in federal court also requires demonstrating a "causal connection between the injury and the conduct complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court."[105] Hackers cannot violate individuals' constitutional rights—only state and local officials can. Depending on the scenario, the election officials who manage a system compromised by a security breach have potentially violated voters' rights by conducting the election using an insecure system, failing to ensure the accuracy of the voter records and vote counts, including altered or erroneous votes in the final tallies, or certifying election results that effectuate the disenfranchisement of otherwise qualified voters. The injury suffered by voters (the deprivation of the right to cast an effective ballot) is fairly traceable to the conduct and administration of an election voting system in a manner that disenfranchises qualified voters. And, in certain circumstances, even if election officials could be said to be "only implementing the consequences of others' actions," a voter would still have standing to sue those officials "for their actions in carrying out those consequences."[106]

Only public elections officials have the power to redress the violations at issue by taking steps to ensure the accurate and effective counting of ballots and ensuring the validity of the election results, even if that means reforming the vote counts or even re-running the election. A court order, for example, prohibiting certification of the election results undermined by hacking and requiring a recount, revision, or special election—"a change in [the] legal status" of the putative results— would, as a practical consequence, provide redress.[107] Under such circumstances, courts generally find standing.[108]

B. Potential Defendants

The Eleventh Amendment generally provides states with immunity against civil suits, including suits to enforce federal rights. For this reason, defendants in election cases are typically the individual public officials responsible for the voting system at issue, sued in their official capacity for declaratory or injunctive relief only.[109] Where a party seeking to protect the vote seeks relief from the problematic effects of a hacked election—whether on federal constitutional or other grounds—the appropriate defendant will depend on the nature of the election interference and how responsibility for the relevant election procedure is allocated under state law. States vary in whether they assign responsibility for counting ballots, certifying election results, and ensuring compliance with federal and state election laws to state or local officials. Thus, the analysis will always be state-specific.

C. Evidentiary and Discovery Considerations

Any post-election effort to remedy the effects of hacking, including litigation, will be fast-paced and somewhat chaotic. This section highlights the kinds of evidence and discovery that may be both important and feasible to acquire within the compressed timeframes available in such efforts. This discussion is not comprehensive.

1. Evidence Available Without Discovery

Given the condensed timeframes involved, successful post-election strategies for protecting voters' rights in the face of a possible hack require supporting evidence that can be quickly gathered and presented to elections officials or the court. Much of this information can be gathered separate and apart from formal discovery.

a. Experts

Declarations and testimony from a variety of experts could be critical in a post-election challenge to a hacked election.

<u>Computer science and election security</u> experts could provide analysis or testimony about:

- The relevant election system's cyber-security flaws;

- The history of public warnings about these vulnerabilities, including past expert or scholarly analyses, studies, or publications, showing the extent to which elections officials may or should have been aware of those vulnerabilities and the ease with which those vulnerabilities could have been mitigated;

- Explanations of how and why available information about problems with the election (e.g., strange vote totals, reports of missing races on individual voters' ballots, reports that voters showed up to vote but were not on the official voter rolls, etc.) suggest that a hack has in fact taken place. If there is no "smoking gun" evidence immediately available (e.g., an announcement from a hacker taking credit for hacking the election, or confirmation from elections officials that their systems have been hacked), then testimony from computer science and election security experts analyzing the available information and explaining how that information is indicative that a hack has occurred could be critical; and

- The kinds of information that could be retrieved from the voting machines or systems that would help determine the nature and extent of any hack. For example, expert testimony regarding how voting machines or systems could be forensically examined and what such an examination would show would likely be critical to help a court determine whether to order such an examination.

Statistical experts may be able to demonstrate whether any hacking is likely to have affected the outcome, or had a substantial impact on the election, depending on the applicable standard. Statistical experts could explain the level of uncertainty created by available evidence of problems and could provide testimony that would help frame and target further discovery designed to determine whether other evidence is available of hacking that might be outcome-determinative, or that might otherwise meet another standard for post-election challenges.

Election administration experts—including current or former election administration officials in the relevant jurisdiction, if available—may provide useful testimony describing the vulnerabilities of current election systems, alternatives that are more secure, steps that the jurisdiction at issue has or has not taken in the past to address these vulnerabilities, and sources of information that are available in the jurisdiction that might be the subject of expedited targeted discovery. Current or former election officials from other jurisdictions may also provide useful testimony, in particular if their jurisdiction has used the election systems at issue.

National security experts could provide testimony explaining the threat of hacking and the available evidence that hacking has been attempted or in fact has occurred. As discussed below, however, there is already substantial evidence in the public domain regarding the serious threat of hacking that our nation's election systems face.

b. Public Reports and Data

Along with expert testimony, publicly available reports, data, and statements could provide useful evidence in a post-election challenge. Many state-commissioned reports and scholarly articles have identified numerous cyber-vulnerabilities in a variety of election systems. For example, both Ohio and Maryland commissioned assessments of the reliability of Premier's (former Diebold's) election systems.[110] National security officials and experts have also made repeated public statements and reports identifying and highlighting the increased threat of hacking that our nation's election systems face.[111]

Publicly reported election returns may also provide a source of evidence that hacking (or other tabulation errors) have occurred. Expert analysis of public data to identify strange results that may be evidence of hacking will likely be a critical part of post-election litigation.

c. Individual Voters

Declarations from individual voters about their experiences having problems related to voting will likely be another source of evidence. For example, courts have relied on individual voter declarations that they received the wrong ballot, that voting machine did not function properly, or that they did not appear on the voter rolls despite having registered to vote, as important evidence in litigation challenging vulnerable election systems.[112] Declarations from multiple voters who experienced similar problems could provide important support for claims that systematic hacking occurred, and could be relevant to requests for targeted discovery designed to reveal additional evidence of systematic problems.

d. Other Sources of Relevant Information

Because of the limited time available to conduct formal discovery, other sources of information should be explored. In particular, state and local public records requests could provide a speedy mechanism to receive relevant data and information on a faster timeline, in some circumstances, than through formal discovery.

2. Evidence Obtainable Through Expedited Discovery

The traditional rules and timelines of civil discovery do not easily lend themselves to the fast-paced context of post-election litigation. This section discusses overarching considerations of timing and confidentiality concerns applicable to most discovery in this context and highlights potential sources of relevant discovery.

a. Timing and Confidentiality Issues

The particular rules and procedures governing discovery will depend on the court in which the litigation is filed. We discuss the federal standards below, but it is important to recognize that state court procedural rules vary, and in some states statutes specifically address discovery in the context of election contests, often requiring expedited and relevant discovery.[113]

Timing. For any discovery to be useful in this context, it will need to be expedited. Federal district courts vary in the formal standard they apply to requests for expedited discovery, but generally they may order expedited discovery if there is good cause to do so.[114] Good cause is likely to exist in a post-election challenge, given the short deadlines for certifying election results. The more targeted the discovery request, the more likely courts will be to agree that it should be expedited.

Confidentiality. Discovery related to vote counts, voters' registration information, and the software and hardware used to administer an election is likely to raise privacy and confidentiality concerns. For example, election systems vendors have previously objected to public examination of their hardware or software, on the grounds that it is proprietary.[115] Data related to actual votes or individual voter registration may implicate privacy concerns. Given the necessary fast pace, one mechanism to address these concerns with minimal delay could be through a stipulated protective order that keeps sensitive information produced in discovery confidential and requires that confidential information be filed (at least initially) under seal.[116]

b. Likely Sources of Discoverable Information

Some categories of targeted expedited discovery that could be considered in a post-election challenge include the following:

Forensic examination of voting system and voter registration hardware and software (i.e., voting machines, election management system, and/or voter registration databases and pollbooks). Litigants could request that actual voting machines be made available for forensic examination, either by an agreed-upon neutral expert or by the parties' experts. Similarly, the court could permit forensic examination of the jurisdiction's election management system, the state's voter registration database, or precinct-level pollbooks (which might be paper or electronic). These forensic examinations could provide critical information about the likelihood and scope of any hack, including evidence of tampering, internal audit logs, the presence of malware or unauthorized software, or other technical information that would only be available through examining the hardware and software used to administer the election. Given the sensitive nature of this information, a party seeking this discovery would likely be required to seek a court order and a protective order protecting the results from authorized disclosure would likely be necessary.

Examination of paper records of the vote. Where election systems use paper ballots or a printed paper trail, discovery seeking review or analyses of the physical ballots/print-outs could provide evidence of problems with vote tabulation and of whether such problems are substantial and create sufficient uncertainty about the result to require relief. Recounts and post-election audits would rely on examination by election officials of these paper records. Discovery of a sample of these records could provide evidence necessary to support a request for relief requiring a full audit or recount.

Requests for documents, including electronically stored information, from state and local officials responsible for election administration. In addition to evidence from the voting and registration systems themselves, other documents may contain evidence demonstrating the effects of hacking, including documents relevant to voter registration (including state DMV records), communications among elections officials, information from any outside security consultants, or records of voter complaints. Likewise, documents could help demonstrate the history of the voting system, equipment and software in use in the particular jurisdiction, and elections officials' knowledge (if any) of security flaws and actions or failures to act to address known problems.

Depositions of state and local officials responsible for election administration. While litigants often seek and review documents before conducting depositions in the normal course of civil discovery, the compressed timeframes at issue in a post-election hacking-based challenge may make an orderly sequencing of discovery impractical. Depositions of key elections officials may provide a method for eliciting information that is faster and both more expansive and more targeted than may be possible through expedited document requests.

CONCLUSION

Protecting the right to vote and the integrity of our democratic process by securing electronic voting systems against cyber-attack must remain a priority of the highest order. Our hope is that the scenarios addressed in this paper remain hypothetical. However, should they not be, an orderly, rapid, and clear-headed approach to navigating the many issues discussed here will become critical—not just to the resolution of a given race, but to the integrity of the democratic enterprise as a whole.

[1] *See generally* Amicus Curiae Brief of Common Cause, National Election Defense Coalition, and Protect Democracy in *Donna Curling, et al. v. Brian Kemp, et al.*, No. 1:17-cv-02989-AT (N.D. Ga.) (July 17, 2018) (documenting risks to electronic voting systems generally, and Georgia's in particular), *available at* https://www.commoncause.org/wp-content/uploads/2018/07/240-1-Amicus-Brief.pdf; Complaint, *Frank Heindel, et al. v. Marci Andino, et al.*, No. 3:18-cv-01887-DCC (D.S.C.) (July 10, 2018) (same, discussing South Carolina), *available at* https://www.documentcloud.org/documents/4594073-Heindel-v-Andino-FINAL-FILED.html; *see also, e.g.*, Kim Zetter, "The Crisis of Election Security," *New York Times Magazine* (Sept. 26, 2018), *available at* https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html?module=inline.

[2] "In 2016, cyber actors affiliated with the Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure" in at least 18 states, "scanned databases for vulnerabilities, attempted intrusions," and in some cases "successfully penetrated a voter registration database." Senate Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations* at 1 (May 8, 2018), *available at* https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf. In recent testimony to the Senate, the directors of the CIA, FBI, NSA, Defense Intelligence Agency, and National Geospatial Intelligence Agency unanimously agreed "that Russia interfered in the 2016 election, and that the Kremlin will continue to intervene in future elections." Jeremy Herb, "US Intel Chiefs Unanimous That Russia is Targeting 2018 Elections," *CNN* (Feb. 13, 2018), *available at* https://www.cnn.com/2018/02/13/politics/intelligence-chiefs-russia-2018-elections-target/index.html; *see also* Amicus Brief in *Curling v. Kemp*, *supra* note 1, at 12-19 (discussing current threats).

[3] *E.g.*, U.S. Election Assistance Commission, *Election Security Preparedness*, *available at* https://www.eac.gov/election-officials/election-security-preparedness/.

[4] *Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886); *Wesberry v. Sanders*, 376 U.S. 1, 17 (1964) ("No 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. Other rights, even the most basic, are illusory if the right to vote is undermined."); *Gray v. Sanders*, 372 U.S. 368, 381 (1963) ("[t]he conception of political equality from the Declaration of Independence, to Lincoln's Gettysburg Address, to the Fifteenth, Seventeenth, and Nineteenth Amendments can mean only one thing—one person, one vote").

[5] States that currently use paperless direct recording electronic voting machines ("DREs") statewide are Georgia, South Carolina, Delaware, New Jersey, and Louisiana. Nine other states (Florida, Indiana, Kansas, Kentucky, Mississippi, Oklahoma, Pennsylvania, Tennessee, and Texas) use paperless DRE machines in some parts of the state. *See* Verified Voting Verifier, *available at* https://www.verifiedvoting.org/verifier/.

[6] Officials have confirmed, for example, that in 2016 hackers breached the voter registration database in Illinois. "Russians Likely Hacked Illinois Voter Database, Officials Say," *CBS Chicago* (July 13, 2018), *available at* https://chicago.cbslocal.com/2018/07/13/illinois-voters-hacked-russia/.

[7] *See* U.S. Const. Art. I, Sec. 4 ("times, places and manner" of elections for Congress regulated by states, though Congress may make or alter such regulations).

[8] For cases regarding the Equal Protection Clause, *see, e.g.*, *Bush v. Gore*, 531 U.S. 98 (2000); *Burdick v. Takushi*, 504 U.S. 428 (1992); *Reynolds v. Sims*, 377 U.S. 533 (1964); *Gray v. Sanders*, 372 U.S. 368 (1963); the Due Process Clause, *see, e.g.*, *Anderson v. Celebrezze*, 460 U.S. 780 (1983); the First Amendment, *see Anderson*, 460 U.S. at 789; *Tashjian v. Republican Party of Connecticut*, 479 U.S. 208,

(1986); for Article I, Section II, *see United States v. Classic*, 313 U.S. 299, 314-15 (1941); *Wesberry*, 376 U.S. at 17-18.

[9] 52 U.S.C. § 20901 *et seq*. (HAVA); 52 U.S.C. § 20501 *et seq*. (NVRA); 52 U.S.C. § 10101 *et seq.* (VRA).

[10] *Infra* § I.C; *Storer v. Brown*, 415 U.S. 724, 730 (1974) ("[T]here must be a substantial regulation of elections if they are to be fair and honest and if some sort of order, rather than chaos, is to accompany the democratic processes."); *League of Women Voters of Fla., Inc. v. Detzner*, 314 F. Supp. 3d 1205, 1215 (N.D. Fla. 2018) ("Voting also requires extensive administration, planning, and logistics").

[11] *Infra* § I.C.

[12] *Anderson*, 460 U.S. at 787 (emphasis added) (internal quotation omitted); *see Classic*, 313 U.S. at 315 (Constitution protects the "right of qualified voters within a state to cast their ballot and have them counted"); *United States v. Saylor*, 322 U.S. 385, 388 (1944) (recognizing "the elector's right intended to be protected is not only that to cast his ballot but that to have it honestly counted"); *United States v. Mosley*, 238 U.S. 383, 386 (1915); *see also Bush*, 531 U.S. at 104-05 (2000); *Hunter v. Hamilton Cty. Bd. of Elections*, 635 F.3d 219, 234 (6th Cir. 2011) ("'[t]he right to vote includes the right to have one's vote counted on equal terms with others'") (quoting *League of Women Voters v. Brunner*, 548 F.3d 463, 476 (6th Cir. 2008)).

[13] *Burdick*, 504 U.S. at 441.

[14] *See Crawford v. Marion Cty Bd. of Elections*, 553 U.S. 181, 189-90 (2008); *Burdick*, 504 U.S. at 434; *Anderson*, 460 U.S. at 787-89; *Bullock v. Carter*, 405 U.S. 134, 145-46 (1972); *Dunn v. Blumstein*, 405 U.S. 330, 336 (1972). This balancing test, known as the *Burdick* balancing test, and is used to weigh the constitutional significance of state-imposed burdens on the right to vote.

[15] *Burdick*, 504 U.S. at 434 (internal quotations omitted); *see also Crawford*, 553 U.S. at 189-90 (plurality), 205 (Scalia, J., concurring).

[16] *Crawford*, 553 U.S. at 190 (quoting *Norman v. Reed*, 502 U.S. 279, 288-89 (1992)).

[17] *Id.* at 191 (quoting *Norman*, 502 U.S. at 288-89).

[18] *See, e.g.*, *id.* at 189 (plurality) ("[E]ven rational restrictions on the right to vote are invidious if they are unrelated to voter qualifications" and warrant stricter scrutiny.); *Harper v. Va. State Bd. of Elections*, 383 U.S. 663, 666-67 (1966); *Carrington v. Rash*, 380 U.S. 89 (1965) (holding that although Texas is free to take reasonable steps to solve "special problem" of determining service member domicile, "[t]here is no indication in the Constitution that occupation affords a permissible basis for distinguishing between qualified voters within the State[,]" and ban on servicemember voter registration is impermissible burden).

[19] *See Crawford*, 553 U.S. at 197-98 (plurality); *id.* at 204 (Scalia, J., concurring); *Burdick*, 504 U.S. at 435.

[20] *Storer*, 415 U.S. at 730 (There is "no litmus-paper test for separating those restrictions that are valid from those that are invidious[.]"); *Crawford*, 553 U.S. at 191 (plurality).

[21] *See, e.g.*, *League of Women Voters of Ohio*, 548 F.3d at 469 (voting system riddled with errors, including mis-calibrated electronic voting machines); *Common Cause S. Christian Leadership Conference of Greater L.A. v. Jones*, 213 F. Supp. 2d 1106, 1108-10 (C.D. Cal. 2001) (punch-card ballots less reliable than alternative procedures).

[22] Any factual scenario implicating elections for U.S. Representative or Senator would also involve Article 1, Section 2 and the Seventeenth Amendment. With respect to the right to vote for congressional office, "[o]ur Constitution leaves no room for classification of people in a way that *unnecessarily abridges*" the right to vote in federal congressional elections, which right is separately protected by Article I, Section 2 of the U.S. Constitution and by the Seventeenth Amendment. *Wesberry*, 376 U.S. at 17-18 (emphasis added); *see Classic*, 313 U.S. at 314-15 (destruction of ballots and alteration of votes violates Constitution); *see also Saylor*, 322 U.S. at 387, 389 (holding that ballot box stuffing in a Congressional election is a violation of a "right or privilege secured . . . by the Constitution or laws of the United States); *Mosley*, 238 U.S. at 386 (finding the right to vote for members of Congress and "to have one's vote counted" constitutionally protected). Recent cases have not discussed the substantive standard to be applied to determine the scope of an "unnecessary" abridgement in the context of these provisions' protection for congressional voting, or whether these protections are co-extensive with the Fourteenth Amendment.

[23] *See, e.g.*, *Stewart v. Blackwell*, 444 F.3d 843, 868 (6th Cir. 2006) (suggesting strict scrutiny applies were votes are flipped or deleted), *vacated* (July 21, 2006), *superseded*, 473 F.3d 692 (6th Cir. 2007) (defendants ceased using challenged voting system, rendering case moot).

[24] *See supra* n. 6 (2016 breach of Illinois registration database).

[25] *E.g.*, *Parra v. Neal*, 614 F.3d 635, 637 (7th Cir. 2010) (candidate disqualified four days prior to election, when there was no time to remove candidate name from ballot and election officials took all possible steps to notify voters); *Gold v. Feinberg*, 101 F.3d 796, 798-802 (2d Cir. 1996) (challenge to inadvertent late delivery of election machines, failure to remove ineligible candidate from some ballots, and tabulation error); *but see Lakes v. Estridge*, 172 S.W.2d 454, 456 (Ky. 1943) (under state constitutional provision, omission of candidate's name from subset of ballots invalidated election).

[26] *E.g.*, *NEOCH*, 696 F.3d at 597; *Warf v. Bd. of Elections of Green Cty., Ky.*, 619 F.3d 553, 559 (6th Cir. 2010); *League of Women Voters*, 548 F.3d at 478.

[27] *Warf*, 619 F.3d at 559.

[28] *NEOCH*, 696 F.3d at 597-98 (poll worker error in providing wrong precinct ballots resulting in vote disqualification violated due process); *Griffin v. Burns*, 570 F.2d 1065, 1074, 1078-79 (1st Cir. 1978) (finding that Rhode Island's post-election invalidation of absentee ballots violated due process, because voters relied on state directives allowing such ballots); *see also Hoblock v. Albany Cty. Bd. of Elections*, 487 F. Supp. 2d 90, 97 (N.D.N.Y. 2006) ("[W]hen a group of voters are handed ballots by election officials that, unsuspected by all, are invalid, and then state law forbids counting the ballots, the election officials violate the constitutional rights of the voters, and the election process is flawed.") (internal quotations and alterations omitted).

[29] *See, e.g.*, *Bennett v. Yoshina*, 140 F.3d 1218, 1226 (9th Cir. 1998); *Griffin*, 570 F.2d at 1075-76; *Ron Barber for Congress v. Bennett*, 2014 WL 6694451 at *6-7 (D. Ariz. Nov. 27, 2014).

[30] *Griffin*, 570 F.2d at 1077 ("[L]ocal election irregularities, including even claims of official misconduct, do not usually rise to the level of constitutional violations where adequate state corrective procedures exist."); *see also Gold*, 101 F.3d at 801-02.

[31] *Bennett*, 140 F.3d at 1225-26 (collecting cases); *Griffin*, 570 F.2d at 1076-77.

[32] *Ury v. Santee*, 303 F. Supp. 119, 124, 126 (N.D. Ill. 1969).

[33] *League of Women Voters*, 548 F.3d at 478 (stating that possibility that selections "jumped" from chosen candidate to another candidate on DRE implicated substantive due process if it occurred on significant scale).

[34] *NEOCH*, 696 F.3d at 586 (finding that although the number and frequency of voter disqualifications resulting from poll worker error varied from "county to county, the problem as a whole is systemic and statewide").

[35] *League of Women Voters*, 548 F.3d at 478.

[36] *Bush*, 531 U.S. at 104-05; *Dunn*, 405 U.S. at 336 ("[A] citizen has a constitutionally protected right to participate in elections on an equal basis with other citizens in the jurisdiction."); *Hunter*, 635 F.3d at 234 ("[T]he right to vote is protected in more than the initial allocation of the franchise. Equal protection applies as well to the manner of its exercise.").

[37] *E.g.*, *NEOCH*, 696 F.3d at 598 (disparity between voters granted rights under federal consent decree and rest of electorate raises equal protection concerns).

[38] *Bush*, 531 U.S. at 104-05; *see also League of Women Voters*, 548 F.3d at 477 ("At a minimum, . . . equal protection requires 'nonarbitrary treatment of voters.'") (quoting *Bush*, 531 U.S. at 105); *Harper*, 383 U.S. at 666-67.

[39] *League of Women Voters*, 548 F.3d at 477 (citing *Bush*, 531 U.S. at 105); *Stewart*, 444 F.3d at 861 (finding equal protection violation where "through no failure on their parts, Ohio voters facing deficient technology approach the ballot in a position unequal from the portion of the electorate using adequate technology"), *vacated and superseded as moot*, 473 F.3d 692.

[40] *See, e.g.*, *Ury v. Santee*, 303 F. Supp. 119 (N.D. Ill. 1969) (invalidating election where local government had consolidated 32 precincts into six, with vastly different numbers of voters assigned to each, leading to overcrowding and lines that made voting logistically challenging or impossible).

[41] 52 U.S.C. §§ 20507(a)(3), (c), (d). The NVRA "limits the methods which a state may use to remove individuals from its voting rolls and is meant to ensure that eligible voters are not disenfranchised by improper removal." *U.S. Student Ass'n Found. v. Land*, 546 F.3d 373, 381 (6th Cir. 2008). Among the purposes of the NVRA are "to protect the integrity of the electoral process" and "to ensure that accurate and current voter registration rolls are maintained." 52 U.S.C. §§ 20501(b)(3)-(4).

[42] 52 U.S.C. § 20507(b)(2).

[43] 52 U.S.C. § 20510(b).

[44] 52 U.S.C. § 21083(a)(2)(A); *Colon-Marrero v. Velez*, 813 F.3d 1, 21-22 (1st Cir. 2016) (HAVA § 303(a) gives rise to an individual cause of action under §1983 where a voter has been improperly removed from the rolls); *see also Sandusky Cty Democratic Party v. Blackwell*, 387 F.3d 565 (6th Cir. 2004).

[45] 52 U.S.C. §§ 21081 (HAVA § 301), 21083 (HAVA § 303). With respect to voter registration records, in addition to the prohibition on removing voters discussed above, HAVA also imposes express technical security requirements, including that state or local officials "shall provide adequate technological security measures to prevent the unauthorized access to the computerized [voter registration] list." 52 U.S.C. § 21083(a)(3).

[46] *See, e.g.*, *Crowley v. Nevada ex rel. Nevada Sec'y of State*, 678 F.3d 730, 736 & n. 4 (9th Cir. 2012) (holding that "the statutory language of HAVA § 301 clearly does not confer private rights on voters or candidates seeking recounts in local elections," and noting that "case law casts doubt on [the]

assumption" that HAVA might create a private right of action for any other litigants); *Paralyzed Veterans of Am. v. McPherson*, No. C 06-4670 SBA, 2006 WL 3462780, at *10 (N.D. Cal. Nov. 28, 2006) (holding HAVA § 301 not enforceable through 42 U.S.C. § 1983, although "a close, difficult question"); *Taylor v. Onorato*, 428 F. Supp. 2d 384, 387 (W.D. Pa. 2006) (finding no private right of action to enforce HAVA § 301). HAVA also requires, as a condition of receipt of federal funding, that states set up a complaint process that permits any person who believes the minimum technical standards have been violated to file a complaint, and requires the state to provide an "appropriate remedy." 52 U.S.C. §§ 21112(a)(2)(B) and (F). It is beyond the scope of this paper to investigate and assess any state statutory complaint procedures enacted to comply with HAVA. In addition, some state statutes impose detailed security and administrative requirements on state elections systems, some of which can be enforced through litigation. *See, e.g.*, *Chavez v. Brewer*, 214 P.3d 397, 406 (Ariz. Ct. App. 2009) (holding state electronic voting equipment statutes were enforceable through private right of action). Analysis of potential remedies that might be available under such state statutes is also beyond the scope of this paper.

[47] Joshua A. Douglas, *The Right to Vote Under State Constitutions*, 67 Vand. L. Rev. 89, 102 (2014). Arizona grants the right to vote implicitly. *See* Ariz. Const. Art. 7 § 2.

[48] Douglas, *supra* note 49.

[49] *See, e.g.*, *Applewhite v. Commw.*, No. 330 M.D.2012, 2014 WL 184988, at *64 (Pa. Commw. Ct. Jan. 17, 2014) (holding that *Crawford* did not control challenge to Pennsylvania's voter ID law); *Weinschenk v. State*, 203 S.W.3d 201, 212 (Mo. 2006) (observing that "voting rights are an area where our state constitution provides greater protection than its federal counterpart").

[50] *Gunaji v. Macias*, 31 P.3d 1008, 742 (N.M. 2001).

[51] *Wallbrecht v. Ingram*, 175 S.W. 1022, 1026-27 (Ky. 1915).

[52] *Lakes*, 172 S.W.2d at 454.

[53] *Hillard*, 172 S.W.2d at 456.

[54] *Ferguson v. Rohde*, 449 S.W.2d 758, 760 (Ky. 1970).

[55] *See, e.g.*, *MacGuire v. Houston*, 717 P.2d 948, 954-55 (Colo. 1986) (holding that Colorado constitution does not preclude limiting eligibility to serve as election judges to major party affiliates); *Sonneman v. State*, 969 P.2d 632, 638 (Alaska 1998) (adopting *Burdick* framework in case challenging constitutionality of statute ending the practice of rotating the order of candidates' names on ballots).

[56] *Compare* Miss. Code. Ann. § 23-15-923 (allowing any "person desiring to contest the election of another" to bring a challenge) *with* 10 ILCS 5/23-1.2a (allowing only candidates, persons who filed declaration of intent to be write-in candidates, or voters "in a number no less than the largest number of signatures required to nominate a person to be a candidate" to challenge elections) and *Fouts v. Bolay*, 795 So.2d 1116, 1117 (Fla. Dist. Ct. App. 2001) (stating that "quo warranto" action under Fla. Stat. § 80.01 may only be brought by petition who "was the candidate lawfully chosen by the voters for the office in dispute" (quoting *State ex rel. Clark v. Klingensmith*, 163 So. 704 (1935)).

[57] *See, e.g.*, Tex. Elec. Code Ann. § 221.002 (Vernon 1986) (state senate).

[58] *E.g.*, *State ex rel. Leneghan v. Husted*, No. 2018-0866, 2018 WL 4026333, at *5-6 (Ohio Aug. 23, 2018) (applying, in the absence of explicit statutory authorization and under court's mandamus authority, state election law to challenge of federal congressional election); Ohio Rev. Code Ann. § 3515.08.

[59] *E.g.*, Tex. Elec. Code Ann. § 221.001 (Vernon 1986).

[60] *E.g.*, Ga. Code Ann. §§ 21-2-522(1), (3) (result may be contested on ground that "illegal votes have been received or legal votes rejected at the polls sufficient to change or place in doubt the result" or where officials engaged in "misconduct, fraud, or irregularity"); Va. Stat. § 24.2-803(B)(ii) (contest may be based on "objections to the conduct or results of the election accompanied by specific allegations which, if proven true, would have a probable impact on the outcome of the election").

[61] La. R.S. § 18:1432(A) (election may be voided if "it is impossible to determine the result," or if the number of qualified voters denied the right to vote, or unqualified voters who were allowed to vote, or combination of the two "was sufficient to change the result in the election").

[62] *Jenkins v. Williamson-Butler*, 883 So. 2d 537, 540 (La. Ct. App. 2004) (quoting *Adkins v. Huckabay*, 755 So. 2d 206, 222 n. 21 (La. 2000)).

[63] *Jenkins*, 883 So. 2d at 540 (citing *Savage v. Edwards*, 728 So. 2d 428 (La. App. 3 Cir. 1998)).

[64] *Rossano v. Townsend*, 9 S.W.3d 357, 361-62 (Tex. App. 1999) (citing Tex. Elec. Code Ann. § 221.003 (Vernon 1986)).

[65] *Fouts*, 795 So.2d at 1118.

[66] *E.g.*, 29 C.J.S. Elections § 523 *et seq.*; 3 McQuillin Law of Mun. Corp. § 12:54 (3d ed.); Citizens for Election Integrity Minnesota, "State Recount Laws Searchable Database," *available at* https://ceimn.org/searchable-databases/recount-database; Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 Fordham L. Rev. 1711, 1817-36 (2005); Steven F. Huefner, *Remedying Election Wrongs*, 44 Harv. J. on Legis. 265, 270-71 (2007).

[67] *Infra* § II.E.

[68] Constitutional violations that impact elections for President and Vice President raise additional issues, for reasons both logistical and legal. How to assess whether violations have had an outcome-determinative impact on the vote, in light of the nature of the Electoral College, is a substantial issue. As a practical matter, the timing of sending electors to the Electoral College will significantly impact procedural and remedial options. Most significantly, whether a Presidential election can ever be re-run in whole or in part is a question of significant complexity. These issues are beyond the scope of this paper.

[69] *See supra* note 68; *see also, e.g.*, Peter Nicolas, *Electoral Evidence*, 69 Ala. L. Rev. 109, 110 (2017).

[70] *See, e.g.*, *Stein v. Cortes*, 223 F. Supp. 3d 423, 427-30 (E.D. Pa. 2016) (denying preliminary injunction in federal court action and discussing multiple pending state court election contest and recount actions).

[71] *See* Citizens for Election Integrity Minnesota, "State Recount Laws Searchable Database," *available at* https://ceimn.org/searchable-databases/recount-database.

[72] For example, a margin of less than 0.5% triggers a recount in Florida using automatic tabulating equipment; if the margin after this is equal or less than 0.25%, a manual recount of overvotes and undervotes, open to the public, is commenced. Fla. Stat. §§ 102.141(7), 102.166(1).

[73] Georgia, for example, provides for "recounts" of absentee ballots or in those precincts where paper ballots were used, either at the discretion of the superintendent of elections in cases of discrepancy or upon request by a candidate at taxpayers' expense where the difference between the winning candidate and any other candidate is less than one percent of the total votes cast. GA Code § 21-2-495(a), (c)(1). Where votes are cast via electronic voting machine, however, three electors or the superintendent may conduct a "recanvass of the votes shown" on a machine suspected of malfunctioning. GA Code § 21-2-495(b).

[74] Colorado requires every county to conduct a risk-limiting audit of election results after each election. Co. St. §§ 1-7-514, 515. North Carolina requires consultation with a statistician to select a sample size for a manual recount that will produce statistically significant results. N.C. Gen. Stat. § 163A-1166. Wisconsin requires that audits include a sample from each type of voting equipment used in the state. Memorandum from Megan Wolfe, Interim Administrator, Wisconsin Elections Commission, to Municipal, County, and City Clerks of Wisconsin, "2018 Post-Election Voting Equipment Audit," October 1, 2018, *available at* https://elections.wi.gov/sites/default/files/memo/20/commission_sep_25_meeting_audit_decision_10_01_18__29601.pdf.

[75] Florida, for example, requires each county conduct either an automatic and manual audit within seven days of every election; a manual audit reviews one race in 1-2% of precincts, whereas an automatic audit will retally votes cast in every race in at least 20% of randomly selected precincts. Fla. Stat. § 101.591. There is, however, no statutory guidance for what happens if this audit reveals significant discrepancies.

[76] Alaska's audit statute triggers a recount if there is a discrepancy of more than 1% between the hand recount and the count certified by the election board. Alaska Stat. § 15.15.430. North Carolina requires a manual recount if the "discrepancy . . . is significant." N.C. Gen. Stat. § 163A-1166(b)(1).

[77] For example, *Hunter*, 635 F.3d at 247 involved a very close Ohio election for juvenile court judge that turned on the outcome of provisional ballots that were rejected for being cast in the wrong precinct (an issue later addressed again statewide in the *NEOCH v. Husted* and *SEIU Local 1 v. Husted* cases, see *NEOCH v. Husted*, 696 F.3d 580, 592 (6th Cir. 2012)). While the recount was proceeding under state law, the federal court became involved in the conduct of that recount. The Sixth Circuit affirmed the district court's order that the county board "immediately begin an investigation into whether poll worker error contributed to the rejection of the 849 provisional ballots now in issue and include in the recount of the race for Hamilton County Juvenile Court Judge any provisional ballots improperly cast for reasons attributable to poll worker error." *Id.* at 247. The Board was eventually enjoined from "rejecting otherwise valid provisional ballots that were cast in the correct location but wrong precinct," nine ballots determined to be cast in the right precinct, and seven cast due to pollworker error, and ordered to count these ballots in the pending mandatory recounts. *Hunter v. Hamilton Cty. Bd. Of Elections*, 850 F. Supp. 2d 795, 847 (S.D. Ohio 2012); *see also, e.g.*, *Stein v. Thomas*, 222 F. Supp. 3d 539 (E.D. Mich. 2016), *aff'd*, 672 F. App'x 565 (6th Cir. 2016), and *appeal dismissed*, No. 16-2691, 2016 WL 10651059 (6th Cir. Dec. 27, 2016) (issuing preliminary injunction ordering the start of the recount of Michigan presidential vote notwithstanding objections to petition for statutory recount that would normally impose a two-day waiting period so that recount could be completed prior to deadline for naming electors); *Riemers v. Jaeger*, 916 N.W.2d 113 (N.D. 2018) (ordering "automatic recount" pursuant to statute where Secretary of State had failed to conduct it); *In re Election of U.S. Representative for Second Cong. Dist.*, 653 A.2d 79, 89 (Conn. 1994) (referring to court previously ordering an "immediate manual recount" in one county where the result appeared unreliable, despite denying more comprehensive recount).

[78] There may also be disputes about what the relevant deadlines actually are under state law. *See, e.g.*, *Palm Beach Cty. Canvassing Bd. v. Harris*, 772 So. 2d 1273, 1289-90 (Fla. 2000) (construing Florida statutes to determine proper deadlines for recount of votes, in context of 2000 presidential election leading to *Bush v. Gore*).

[79] *LaCaze v. Johnson*, 305 So. 2d 140, 142 (La. Ct. App. 1974). The Louisiana Court of Appeal issued a writ reversing the temporary restraining order, but the next day the Louisiana Supreme Court reversed the Court of Appeal and ordered that the trial court's restraining order be reinstated. *See Lacaze v. Johnson*, 302 So. 2d 613 (La. 1974). The trial court subsequently ordered a re-run election, which the state Supreme Court upheld. *See LaCaze v. Johnson*, 310 So. 2d 86, 87 (La. 1974).

[80] *Tate-Smith v. Cupples*, 134 S.W.3d 535, 537 (Ark. 2003).

[81] *Cf. Ron Barber for Cong. v. Bennett*, No. CV-14-02489-TUC-CKJ, 2014 WL 6694451, at *3-4 (D. Ariz. Nov. 27, 2014) (finding that federal court had jurisdiction over plaintiffs' motion for temporary restraining order to delay certification of vote by Secretary of State, but denying motion for lack of likelihood of success on the merits because plaintiffs had "not shown a pervasive error that undermines the integrity of the vote").

[82] The district court subsequently granted the plaintiffs' motion for summary judgment and entered a permanent injunction but the Second Circuit reversed, concluding that the plaintiffs had not established a federal due process violation. *Shannon v. Jacobowitz*, 394 F.3d 90, 96-97 (2d Cir. 2005), reversing *Shannon v. Jacobowitz*, No. 5:03-CV-1413, 2004 WL 180253, at *1 (N.D.N.Y. Jan. 27, 2004); *see also Rivera-Powell v. New York City Bd. of Elections*, 470 F.3d 458, 465 n. 7 (2d Cir. 2006) (clarifying that election official conduct can trigger due process concerns without officials having "intent actually to interfere with the electoral process").

[83] *See also Application of Bonsanto*, 409 A.2d 290, 293 (N.J. App. 1979) (remanding election contest to trial court for fact-finding as to the validity of specific ballots).

[84] *See Hunter v. Hamilton Cty. Bd. of Elections*, 635 F.3d 219, 247 (6th Cir. 2011) (affirming district court grant of preliminary injunction in part, as to its order that election board investigate certain ballots for poll worker error and count those ballots as required by operative consent decree).

[85] *Hunter*, 850 F. Supp. 2d at 847 (enjoining Board from rejecting specific ballots). Other federal courts have expressed federalism concerns in reviewing specific election outcomes: "We further believe that federal courts are ill-equipped to monitor the details of elections and resolve factual disputes born of the political process. . . . [W]e find sifting the minutae [*sic*] of post-election accusations better suited to the factual review at the administrative and legislative level[.]" *Hutchinson v. Miller*, 797 F.2d 1279, 1286-87 (4th Cir. 1986).

[86] *E.g.*, *Gunaji v. Macias*, 31 P.3d 1008, 1016-17 (N.M. 2001) (rejecting all votes from a precinct); *Matter of Protest Election Returns and Absentee Ballots in November 4, 1997 Election for City of Miami, Fla*., 707 So. 2d 1170, 1174-75 (Fla. 1998) (disregarding all absentee ballots rather than disenfranchise voters who had physically cast a ballot by calling a new election).

[87] *In re Petition to Contest General Election for Dist. Justice in Judicial Dist. 36-3-03 Nunc Pro Tunc*, 670 A.2d 629, 639 (Pa. 1996).

[88] *Gunaji*, 31 P.3d at 1014-16; *Matter of Protest Election Returns*, 707 So.2d 1170; *Bolden v. Potter*, 452 So.2d 566-67 (Fla. 1984) (rejecting all absentee ballots cast where there was evidence of 47 invalid ballots and broader vote-buying scheme).

[89] Some state courts, when confronted with instances where numerous invalid ballots were included among the vote totals, have used "proportional deduction" as a remedy for addressing errors in election administration without requiring a special election. A court using proportional deduction will "for each district in which invalid votes were cast, . . . calculate[] a pro rata deduction of the illegal votes according to the number of votes cast for the respective candidates in that election district." *Huggins v. Superior Court In & For Cty. of Navajo*, 163 Ariz. 348, 352 (1990) (internal quotation omitted); *see Hammond v. Hickel*, 588 P.2d 256, 260 (Alaska 1978); *Clay v. Town of Gilbert*, 773 P.2d 233, 237 (Ariz. Ct. App. 1989). The constitutional implications of the proportional deduction or addition approaches should not be taken lightly, but are beyond the scope of this paper. Note that at least one commentator has suggested that where the number of disputed votes falls within acceptable and demonstrated margins of error, a

resort to the applicable statutory tie-breaker mechanism should be considered. *See* Huefner, *supra* note 68, at 303-04.

[90] *E.g.*, Ind. Code § 3-12-8-17(d), requiring a special election where a candidate was ineligible; a mistake occurred in the printing or distribution of ballots or in the programming of a voting machine, making it impossible to determine which candidate received the highest number of votes; a voting machine or electronic voting system malfunctioned, making it impossible to determine who received the highest number of votes; or a deliberate act or series of actions occurred making that determination impossible.

[91] *Pabey v. Pastrick*, 816 N.E.2d 1138, 1150-51, 54 (Ind. 2004).

[92] *Rogers v. Holder*, 636 So. 2d 645, 651-52 (Miss. 1994).

[93] *E.g.*, *Nageak v. Mallott*, 426 P.3d 930, 940 (Alaska 2018) (noting that in procedural challenges where no fraud or corruption is alleged, challenger must show "the existence of malconduct sufficient to change the results of the election," but where the propriety of certain votes is at issue, "[t]he concept of malconduct does not enter into the question") (quoting *Willis v. Thomas*, 600 P.2d 1079, 1081 (Alaska 1979)); *Walker v. Smith*, 57 So. 2d 166, 166-67 (Miss. 1952) (noting that Mississippi courts distinguish between cases of illegal votes, where a challenger must show those votes altered the outcome, and cases where a "total departure from the statutory requirements" make an election void); *see also Thompson v. Jones*, 17 So. 3d 524, 526 (Miss. 2008) (stating that special election warranted where "enough illegal votes were cast for the contestee to change the result of the election" or "make it impossible to discern the will of the voters") (internal citations omitted); *State ex rel. Leneghan v. Husted*, No. 2018-0866, 2018 WL 4026333, at *6 (Ohio Aug. 23, 2018) (stating that Ohio applies a single standard to procedural and substantive challenges, analyzing whether "the irregularity or irregularities affected enough votes to change or make uncertain the result of the election"); *Flores v. Cuellar*, 269 S.W.3d 657, 660 (Tex. App. 2008) ("To overturn an election, the contestant must prove by clear and convincing evidence that voting irregularities materially affected the election results."); *In re Election Contest as to Watertown Special Referendum Election of Oct. 26, 1999*, 628 N.W.2d 336, 338 (S.D. 2001) ("Contestants must show not only voting irregularities, but also show those irregularities to be so egregious that the will of the voters was suppressed.").

[94] For example, in *Hamer v. Campbell*, 358 F.2d 215 (5th Cir. 1966), the Fifth Circuit ordered election results annulled and a new election run where the elections were conducted in violation of pre-election injunctions concerning racial discrimination in voter registration. *See also Hadnott v. Amos*, 394 U.S. 358 (1969) (ordering district court to declare certain candidates victorious and order a new election as to other races, where qualified candidates were barred from appearing on ballot for various county and state offices); *Bell v. Southwell*, 376 F.2d 659 (5th Cir. 1967) (ordering election results set aside and new election where "gross, state-imposed, and forcibly state-compelled" racial discrimination affected election); *Toney v. White*, 488 F.2d 310 (5th Cir. 1973) (affirming vacation of election results in case of substantial race discrimination affecting election outcome). In *Gjersten v. Board of Election Comm'rs for City of Chicago*, 791 F.2d 472, 479 (7th Cir. 1986), the Seventh Circuit identified a number of factors, in addition to the rights of candidates and voters, which a court ought to consider in deciding whether to call a new election: the integrity of the election system and necessity of continued governance; whether the unconstitutional practice at issue had a significant impact; whether the plaintiffs pursued their claim in a timely fashion, including by filing for pre-election relief, where appropriate; the costs on candidates and local governments of running elections; and the interest in finality and limiting the number of times voters must return to the polls. Other federal courts have explained that they will overturn elections only where "confronted with an officially-sponsored election procedure which, in its basic aspect, was flawed," *Hart v. King*, 470 F. Supp. 1195, 1198 (D. Haw. 1979), or the irregularities were so great that there is a probability—not just the possibility—that they altered the results. *Lehner v. O'Rourke*, 339 F. Supp. 309,

314 (S.D.N.Y. 1971); *see also Powell v. Power*, 320 F. Supp. 618, 622 (S.D.N.Y. 1970), *aff'd,* 436 F.2d 84 (2d Cir. 1970).

[95] *United States v. Hays*, 515 U.S. 737, 742-43 (1995) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)) (internal quotation omitted). We do not address here standing considerations in contexts other than a post-election scenario involving a possible hack; for example, we do not address the pre-election context where risk of a cybersecurity breach is imminent.

[96] *FEC v. Akins*, 524 U.S. 11, 24 (1998); *see also Gray v. Sanders*, 372 U.S. 368, 375 (1963) (individual voter had standing to challenge county unit system for counting vote in primary election for statewide offices).

[97] *See Stewart*, 444 F.3d at 853-55; *Black v. McGuffage*, 209 F. Supp. 2d 889, 895 (N.D. Ill. 2002); *see also Curling v. Kemp*, No. 1:17-cv-02989-AT, 2018 WL 4625653, at *7-11 (N.D. Ga. Sept. 17, 2018) (holding voters had standing in pre-election challenge to unsecure DRE-based voting system, where plaintiffs alleged system had been exposed to outside access on a public server and alleged "a threat of a future hacking event that would jeopardize their votes and the voting system at large," violating "their fundamental right to participate in an election process that accurately and reliably records their votes and protects the privacy of their votes and personal information").

[98] *See Akins*, 524 U.S. at 24-25 ("Widely shared" informational injury resulting from FEC refusal to require AIPAC to disclose campaign spending was "directly related to voting, the most basic of political rights, [and] is sufficiently concrete and specific[.]").

[99] *League of Women Voters of Ohio*, 548 F.3d at 477-78 (holding that where plaintiff alleged voters were forced to stand in line for excessive time, were denied disability-related assistance, were subject to polling places with insufficient machines, and were subject to arbitrary application of provisional ballot procedures, plaintiff had stated claims for equal protection and substantive due process violations sufficient to survive a motion to dismiss).

[100] *E.g.*, *Hamer v. Campbell*, 358 F.2d 215 (5th Cir. 1966) (class of African-American citizens sought injunction preventing and then vacating election where denied the right to vote on basis of race); *Madera v. Detzner*, 325 F. Supp. 3d 1269 (N.D. Fla. 2018) (suit brought on behalf of all Puerto Rico-born eligible voters with limited English proficiency residing in 32 Florida counties).

[101] *Hunt v. Washington State Apple Advertising Comm'n*, 432 U.S. 333, 342-43 (1977); *see, e.g.*, *Partnoy v. Shelley*, 277 F. Supp. 2d 1064, 1072 (S.D. Cal. 2003) (unincorporated association had standing to bring challenge to constitutionality of provision limiting electorate in recall vote on behalf of its members); *Florida Democratic Party v. Hood*, 342 F. Supp. 2d 1073, 1079 (N.D. Fla. 2004) (political party had standing to sue on behalf of members who will vote in upcoming election); *Hancock County Bd. Of Sup'rs v. Ruhr*, 487 Fed. App'x 189, 197-99 (5th Cir. 2012) (NAACP had standing to bring "one person, one vote" challenge on behalf of its members even where they did not identify by name an affected member in the pleadings). The U.S. Supreme Court agreed, without comment, that the Democratic Party had standing to challenge the validity of Indiana's voter ID law in *Crawford*, 553 U.S. at 189 n. 7. *See also Florida Democratic Party v. Scott*, 215 F. Supp. 3d 1250, 1254 (N.D. Fla. 2016) (holding that even though plaintiff organization could not identify specific voters who were affected by governor's refusal to extend registration deadline, "it is sufficient that some inevitably would"); *Bay Cty. Democratic Party v. Land*, 347 F. Supp. 2d 404, 422-23 (E.D. Mich. 2004) (holding that where provision ballots had not been counted in prior elections, "prospect of recurrence at the upcoming general election" was certain and therefore organizational plaintiffs did not need to identify specific members who would be affected).

[102] *See, e.g.*, *Fla. State Conference of the NAACP v. Browning*, 522 F.3d 1153, 1165-66 (11th Cir. 2008). *See also Arcia v. Fla. Sec'y of State*, 772 F.3d 1335, 1340-42 (11th Cir. 2014) (holding that organizations

had standing to sue on their own behalf where they redirected resources from voter registration drives to locate and assist voters removed from the rolls in violation of the NVRA).

[103] *Burdick*, 504 U.S. at 438 (observing that "the rights of voters and the rights of candidates do not lend themselves to neat separation") (quoting *Bullock*, 405 U.S. at 143); *cf., e.g.*, *Hawkins v. Wayne Tp. Bd. of Marion County, IN*, 183 F. Supp. 2d 1099, 1103 (S.D. Ind. 2002) (holding that voters who erroneously received the wrong ballots were deprived of "the opportunity to vote for [plaintiff] that they should have had" and the candidate therefore suffered an injury in fact).

[104] *E.g.*, *Bush v. Gore*, 531 U.S. 98 (2000); *Gamza v. Aguirre*, 619 F.2d 449 (5th Cir. 1980); *Kurita v. State Primary Bd. of Tenn. Democratic Party*, 2008 WL 4601574 (M.D. Tenn. Oct. 14, 2008).

[105] *Lujan*, 504 U.S. at 560-61 (internal citations and alterations omitted).

[106] *Durham v. Martin*, 905 F.3d 432, 434 (6th Cir. 2018).

[107] *See Utah v. Evans*, 536 U.S. 452, 464 (2002).

[108] *Id*.

[109] *E.g.*, *Edelman v. Jordan*, 415 U.S. 651 (1974); *see Ex parte Young*, 209 U.S. 123 (1908); Rochelle Bobroff, *Ex Parte Young as a Tool to Enforce Safety Net and Civil Rights Statutes*, 40 Univ. of Toledo L. Rev. 819 (2009).

[110] Patrick McDaniel, *et al.*, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards, and Testing* 103 (Dec. 7, 2007); Science Apps. Int'l Corp. (SAIC), *Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes* (Sept. 2, 2003).

[111] *E.g.*, Ryan Gardner, *et al.*, "Software Review and Security Analysis of the Diebold Voting Machine Software," Florida State University Security and Assurance in Information Technology (SAIT) Lab Report for Florida Department of State (July 27, 2007), 3-4, 30-35 (listing 126 flaws in Diebold voting systems), *available at* http://nob.cs.ucdavis.edu/bishop/notes/2007-fsusait-2/2007-fldiebold.pdf; John Schwartz, "Computer Voting Is Open to Easy Fraud, Experts Say," *New York Times* (July 24, 2003) (Diebold election system used in Georgia "contains serious flaws that would allow voters to cast extra votes and permit poll workers to alter ballots without being detected"), *available at* https://www.nytimes.com/2003/07/24/us/computer-voting-is-open-to-easy-fraud-experts-say.html; Tadayoshi Kohno, *et al.*, "Analysis of an electronic voting system," *Proceedings - IEEE Symposium on Security and Privacy* (2004), *available at* https://homes.cs.washington.edu/~yoshi/papers/eVoting/vote.pdf; Ariel Feldman, *et al.*, "Security Analysis of the Diebold AccuVote-TS Voting Machine" (Sept. 13, 2006) (finding Diebold machine "vulnerable to extremely serious attacks"), *available at* https://s3.amazonaws.com/citpsite/publications/ts06full.pdf.

[112] *League of Women Voters of Ohio v. Brunner*, 548 F.3d 463, 467-68 (6th Cir. 2008); *Curling*, 2018 WL 4625653, at *7 (listing evidence of ongoing problems based on voter affidavits).

[113] *E.g.*, Ga. Code Ann. § 21-2-525(b) (trial judge may do everything "necessary and proper" to expeditiously hear and resolve election dispute, including "to compel the production of evidence which may be required at such hearing"); 10 Ill. Comp. Stat. Ann. 5/23-1.6a (plaintiffs in statewide election contests may request examinations of "records and equipment under the control of an election authority").

[114] F.R.C.P. 26(d); *e.g.*, *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 276 (N.D. Cal. 2002).

[115] *E.g.*, Jessica Ring Amunson & Sam Hirsch, *The Case of the Disappearing Votes: Lessons from the Jennings v. Buchanan Congressional Election Contest*, 17 Wm & Mary Bill Rts. J. 397, 405-11 (2008),

available at https://jenner.com/system/assets/publications/579/original/HirschAmunson.pdf?1313668446; Kim Zetter, *In Industry First, Voting Machine Company to Publish Source Code*, WIRED Magazine (Oct. 27, 2009), *available at* https://www.wired.com/2009/10/sequoia/.

[116] *See* F.R.C.P. 26(c).