No. 19-1399

IN THE

Supreme Court of the United States

SHELBY ADVOCATES FOR VALID ELECTIONS, ET AL.,
Petitioners,

v.

TRE HARGETT, ET AL.
Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

---

BRIEF OF *AMICI CURIAE* INDIVIDUAL ELECTION SECURITY EXPERTS IN SUPPORT OF CERTIORARI

Courtney Hostetler
Ronald Fein
John Bonifaz
Ben Clements
FREE SPEECH FOR PEOPLE
1320 Centre St. #405
Newton, MA 02459
(617) 249-3015

John D. Graubert
Counsel of Record
Megan C. Keenan
Ryan Miller
Jeremy Patashnik
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
jgraubert@cov.com
(202) 662-6000

July 22, 2020

Counsel for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTERESTS OF *AMICI CURIAE*[1]

Amici curiae are individual election security experts[2] with technical expertise in the security of electronic voting systems. They have an interest in ensuring that legal standards accurately reflect the risks associated with such systems, as well as an interest in ensuring that courts are able to consider challenges to use of voting machines that experts have concluded are error-prone and likely to disenfranchise voters.

---

[1] In accordance with Rule 37.2(a), all counsel of record received timely notification of *amici curiae*'s intent to file this brief and have consented, in writing, to this filing. No party or counsel for a party authored this brief in whole or in part. No party, counsel for a party, or person other than *amici curiae* and their counsel made any monetary contribution intended to fund the preparation or submission of this brief.

[2] A complete list of these experts is provided as an appendix to this brief. *See* App. 1a–2a. Experts' institutional affiliations are included for identification purposes only and do not constitute or reflect institutional endorsement.

SUMMARY OF ARGUMENT

The Sixth Circuit's incorrect interpretation of this Court's imminence requirement to state a case or controversy will extinguish challenges to readily apparent risks of harm in upcoming elections—including harm that experts such as *amici* have determined is inevitable based on an extensive and comprehensive record of technical failures, well-researched and documented systemic weaknesses, and vote-counting errors inherent with the voting machines at issue, the AccuVote-TSx Direct Recording Electronic ("DRE"). This Court's precedent requires that the combination of (a) repeated and well-documented instances of machine malfunctions causing miscounting of votes in Shelby County and beyond and (b) Respondents' failure to respond or remedy these persistent errors is sufficient to plausibly allege a "substantial risk" that the same errors will recur. Despite the impossibility of identifying such harms with *absolute certainty* in advance of an election, courts must be able to intervene to stop well-documented, recurring voting rights violations.

The Sixth Circuit's narrow construction of the imminence requirement warrants this Court's reconsideration. The decision below disregards the substantial risk that recurring technical errors will persist in future elections and overlooks the multiple ways that AccuVote-TSx voting machines have consistently diluted and diminished Tennesseans' fundamental right to vote. First, many technical and scholarly analyses, backed by real-life voter experiences, have found the machines do not record and/or tabulate votes reliably or consistently. Second, the

machines are susceptible to infection by malicious software designed to undetectably misrecord and miscount votes. And third, the full extent of those errors is impossible to track because of the lack of a voter-verified paper ballot. Many of these errors do not turn on the type of human discretion and caution that can prevent reoccurrence, and their persistence in elections for multiple years in multiple locations demonstrates the imminent risk that they will occur again in future elections. The Sixth Circuit avoided this conclusion by understating Petitioners' well-pleaded allegations and overstating the threshold for imminence required by this Court's precedent.

This Court's review is further needed because the decision below creates a circuit split. The Eleventh Circuit has rejected such a cramped interpretation of imminent harm, including in cases involving similar—and even materially identical—facts. And for good reason. The Eleventh Circuit's approach protects the integrity of elections and voters' constitutional rights by permitting courts to intervene when states choose to hold their elections in a manner that has repeatedly resulted in vote dilution or disenfranchisement and fail to remedy the processes that led to those harms. The Sixth Circuit's contrary interpretation of the imminence requirement would prevent courts from considering such claims and safeguarding the fundamental right to vote, which necessitates this Court's immediate review.

ARGUMENT

I. ABSENT IMMEDIATE REVIEW, VOTING MACHINES IN SHELBY COUNTY WILL CONTINUE TO CAUSE FLAWED ELECTIONS.

Shelby County, Alabama
Shelby County, Illinois
Shelby County, Indiana
Shelby County, Iowa
Shelby County, Kentucky
Shelby County, Missouri
Shelby County, Ohio
Shelby County, Tennessee <-
Shelby County, Texas

Shelby County's voting machines have a widespread, well-documented history of vote-counting errors that experts have concluded will recur. Furthermore, these machines suffer from severe security vulnerabilities, rendering them subject to hacking by both foreign and domestic actors. Both of these problems are further exacerbated by the machines' lack of any auditable paper trail, which makes it difficult, if not impossible, to detect and correct vote-counting errors. As a result, the machines used in Shelby County are so unreliable as to pose an imminent threat to voters' rights.

In poorly designed and badly implemented systems that fail to provide sound audit trails, exploiting any weak link is likely to be enough to compromise the entire process. Yet the decision below—which focuses narrowly on the human errors that have plagued Shelby County elections and then deems these problems too speculative to pose an imminent risk under its heightened imminence standard—fails to grapple with the serious technological flaws that have and will continue to jeopardize the validity of elections in Shelby County. *See* Pet. App. 12. The resulting incomplete imminence analysis ignores numerous systematic violations of voters' rights and dismisses

the extensive body of technical research that has established that AccuVote-TSx does not reliably or accurately record and count votes.

A. The Voting Machines At Issue Are Fundamentally Deficient.

A. The Voting Machines At Issue Are Fundamentally Deficient.

The flaws in these voting machines are well documented. Shelby County continues to use the AccuVote-TSx (produced by Premier Election Solutions ("Premier"), formerly Diebold Election Systems ("Diebold")) even though multiple states have concluded that these machines cannot reliably count votes. More than a decade ago, in 2007, the California Secretary of State decertified the AccuVote-TSx after conducting a comprehensive review that concluded the machines "were inadequate to ensure [the] accuracy and integrity of the election results." Cal. Sec'y of State, *Withdrawal of Approval* 2, 3 (Oct. 25, 2007), https://bit.ly/2CA5YEB. The review also found that AccuVote-TSx systems "contain serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes," including by "install[ing] malicious software on voting machines and on the election management system, which could cause votes to be recorded incorrectly or to be miscounted, possibly altering election results." *Id.* at 2. This review further noted that:

> the Diebold system is susceptible to computer viruses that propagate from voting machine to voting machine and even voting machines to the election management system, which could allow an attacker with access to only one voting unit or memory card to spread malicious code,

> between elections, to many, if not all, of a county's voting units.

Id. Perhaps most concerning, the study concluded that such attacks may be difficult if not impossible to detect by audit. *Id.* at 3.

The AccuVote-TSx system's unreliable vote recording and vulnerability to hacking have been repeatedly identified and condemned by other states reviewing this system. Ohio's Secretary of State commissioned an analysis that concluded that flaws in this election system "lead to a broad spectrum of issues that undermine the voting system's security and reliability," and "[t]he resulting vulnerabilities are exploitable by an attacker, often easily so, under election conditions." Patrick McDaniel, et al., *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing* 103 (Dec. 7, 2007), https://bit.ly/2ZJpNCV. Another Ohio study discovered that the memory sources that these machines used to tabulate votes were not even internally consistent. Election Sci. Inst., *DRE Analysis for May 2006 Primary, Cuyahoga County, Ohio* 2 (2006), https://bit.ly/2CdsUGw. That is, although a machine's election archive is supposed to function as an identical back-up copy of its memory card, vote totals reflected on the memory card

can differ from the totals stored in the election archive. *Id.* at 2, 104, 117, 124.[3] Another official assessment commissioned by the State of Maryland likewise identified "several high-risk vulnerabilities" in the Diebold AccuVote-TS system—a similar machine produced by Diebold—and concluded that "[i]f these vulnerabilities are exploited, significant impact could occur on the accuracy, integrity, and availability of election results," and that "[t]he system . . . is at high risk of compromise." Sci. Apps. Int'l Corp., *Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes* ii, v (Sept. 2, 2003), https://elections.maryland.gov/pdf/riskassessmentreport.pdf.

Academic institutions and private organizations have echoed these concerns about the failings and vulnerabilities of the AccuVote-TSx. Scholars at Princeton's Center for Information Technology Policy who analyzed an AccuVote-TS machine found it "is vulnerable to extremely serious attacks." Ariel Feldman, et al., *Security Analysis of the Diebold AccuVote-TS Voting Machine* 1, USENIX/ACCURATE Electronic Voting Technology Workshop (Aug. 2007), https://www.usenix.org/legacy/events/evt07/tech/full_papers/feldman/feldman.pdf. Other scholarship has

---

[3] The study also showed that these electronic memory sources were inconsistent with the paper poll tape produced by voting machines that included an optional printer attachment. *See id.* at 2, 124. The machines used in Shelby County do not use these attachments and thus produce no paper audit trail, which means that Defendants rely exclusively upon the inconsistent, unauditable electronic totals.

produced similarly stark results.[4] One scholar recently demonstrated his ability to manipulate votes cast on an AccuVote-TSx machine in a mock election and explained that malicious actors could do the same thing in a real election by emailing a virus to election officials responsible for programming the machines. Matteen Mokalla et al., *I Hacked an Election. So Can the Russians*, N.Y. Times (Apr. 5, 2018), https://nyti.ms/2IxA5dx (video at 1:18, 1:49–2:30).

Voters have been acutely aware of the machines' tendency to cause "vote flipping,"

The experiences of voters in Shelby County further illustrate the fundamental problems with these machines. Voters have been acutely aware of the machines' tendency to cause "vote flipping," whereby a voter selects her chosen candidate, but the faulty voting machine erroneously records the vote for an opposing candidate. Former Tennessee Attorney General Mike Cody reported that even he had difficulty trying to vote for his preferred congressional candidate in the 2016 federal elections, because the

---

[4] *See, e.g.*, Ryan Gardner et al., Fla. St. Univ. Sec. & Assur. in Info. Tech. Lab., *Software Review and Security Analysis of the Diebold Voting Machine Software: Final Report for Fla. Dep't of State* 6, 30–35 (July 27, 2007), https://web.archive.org/web20080214182346/http://election.dos.state.fl.us/pdf/SAITreport.pdf (listing 126 flaws in Diebold voting systems); John Schwartz, *Computer Voting Is Open to Easy Fraud, Experts Say*, N.Y. Times (July 24, 2003), https://www.nytimes.com/2003/07/24/us/computer-voting-is-open-to-easy-fraud-experts-say.html (noting that the 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"); Douglas Jones & Barbara Simons, *Broken Ballots: Will Your Vote Count?* 164–82, 205–06 (2012) (discussing numerous studies finding serious vulnerabilities in Diebold machines and systems).

voting machine "defaulted or bounced up to the first person on the ballot." Carol Chumney et al., *Voting on Thin Ice: How Systemic Voting Failures Are a Real Threat to Our Democracy* 40–41 (2017), https://bit.ly/2WwHALq. During the 2016 federal elections, Shelby County's AccuVote-TSx DRE systems suffered from touchscreen calibration malfunctions that resulted in votes for one presidential candidate being incorrectly selected as votes for a second presidential candidate, and votes for the second candidate not being selected at all. *Stylus Added to Voting Machine to Help Avoid Vote Flipping,* WMCActionNews5.com (Nov. 1, 2016), https://bit.ly/34tQtH1. Shelby County's Election Commissioner, Norma Lester, expressed concern about the AccuVote-TSx machines being prone to vote flipping, citing "numerous occasions" in the 2016 national presidential election when selecting one candidate caused the machine to flip to the other. Chumney et al., *supra*, at 41. The Shelby County Election Commission's only attempt to fix this problem was to advise voters to use a stylus on these touchscreens. Yet vote-flipping problems continued to plague voters in subsequent elections. Compl. Ex. S at 2, Dist. Ct. Doc. 104-24. In 2018, one voter reported six instances of vote flipping when she tried to cast her ballot using the AccuVote-TSx DRE. *Id.* These well-documented instances of vote-flipping inflict a real and definite injury by frustrating the voting rights of Shelby County voters, and these errors will continue without corrective action.

The Diebold AccuVote-TSx voting system is also prone to lose or alter digitally recorded votes as votes are transferred and aggregated at the county level.

Further analysis has found that the associated Diebold backend database ("GEMS database"), to which votes are uploaded and aggregated from the AccuVote-TSx via memory card, also suffers from multiple critical design flaws. After an election in 2004, technicians discovered that, although Illinois's voting machines had reflected that memory cards were successfully uploaded to the database, *none* of the votes on the memory card had actually been transferred. Lawrence Norden, Brennan Ctr. for Justice, *Voting System Failures: A Database Solution* 10 (2010), https://bit.ly/2ZqPA2w. Election officials in Ohio discovered a similar undetected upload failure again in 2008. *Id.* Diebold initially blamed the error on the presence of antivirus software, but an independent analysis proved it was a logic flaw in the Diebold software. *Id.* at 11. Researchers have also discovered that the backend database is built on outdated Microsoft Jet software that can become corrupted or lose data (i.e., votes) under circumstances that are common in election administration. Thomas P. Ryan & Candice Hoke, *GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standards* 12, USENIX Workshop on Accurate Electronic Voting Technology (Aug. 2007), https://bit.ly/3eN8qFz. For this reason, Microsoft has warned that "because Jet does not use a transaction log (as do the more advanced database systems, such as SQL Server), *it is not possible to reliably prevent any and all database corruption*." Microsoft Support, *How to Troubleshoot and to Repair a Damaged Access 2002 or Later Database* (Apr. 17, 2018), https://bit.ly/2Om6tF1 (emphasis added). Premier (formerly Diebold) has published Product Advisory Notices on these flaws, warning that its product may

fail to properly upload votes to the backend database and might not even display an error message if such a failure occurs. *See, e.g.*, *Product Advisory Notice PAN2008-002* (Apr. 4, 2008), https://bit.ly/2WBVBaK ("The GEMS application has a database file size limit of 2 Gigabytes . . . . This means that the GEMS database file must not reach 2 Gigabytes, otherwise the application will no longer function properly for this database. An error message may or may not be displayed.").

The manufacturer no longer makes the devices used by the County nor services the accompanying software.

Compounding all these issues is the further problem that Shelby County's machines are thoroughly outdated. The manufacturer no longer makes the devices used by the County nor services the accompanying software, meaning that these systematic problems will continue completely unchecked. Even Shelby County has acknowledged that "[t]he absence of vendor support for the critical and obsolescent software presents an unacceptable risk to the election delivery capability." Shelby Cty., *RFQ # 15-008-10 Consultant Services: Replacement of Election System Management Software* (2015), https://rb.gy/n7axe2. This lack of support underscores what experts have already opined: these machines' technical problems will only worsen, not improve, with time. *See* Duncan Buell & Gregory Gay, *Is Technology the Answer? Software Quality Issues in Electronic Voting Systems* 3 (2019), https://bit.ly/36zQBXy (noting that "[h]ardware failures, including screen calibration and timing issues . . . increase[] over time as these systems age").

B. The Voting Machines At Issue Cannot Be Reliably Audited.

B. The Voting Machines At Issue Cannot Be Reliably Audited.

Given these well-documented errors and vulnerabilities with AccuVote-TSx machines, it is imperative that officials in Shelby County be able to conduct a thorough and reliable post-election audit to ensure that votes have not been lost, added, miscounted, or manipulated. But Shelby County's paperless systems are not equipped to meet even this low bar. The only way to review the votes from Shelby County's DREs is by using data recorded by the machines. But if the data itself is corrupted—such as from a software error or intentional interference, to which the system is prone—then the post-election review may not shed light on the underlying problems.[5] *See* P.B. Stark & D.A. Wagner, *Evidence-Based Elections*, 10(5) IEEE Sec. & Privacy 33, 33 (2012), https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf ("[B]ecause paperless voting machines preserve only an electronic record of the vote that cannot be directly observed by voters, there is no way to produce convincing evidence that the electronic record accurately reflects the voters' intent."); *see also* Buell & Gay, *supra*, at 39 (observing that an "inherent

[5] Notably, even the printer attachment offered by the vendor—which Shelby County does not use—to provide a print-out to voters of their choices is not reliable. Harry A. Green et al., Tenn. Advisory Comm'n on Intergovernmental Relations, *Trust But Verify: Increasing Voter Confidence in Election Results* 36 (2007), https://bit.ly/2NgzJO0 (noting that California declined to certify AccuVote-TSx with printer attachment after finding a 10% error rate in mock election with 96 machines).

problem" with an analysis based only on data is that "there is no way to determine ground truth").

"Election audits are critical to ensuring the integrity of election outcomes and for raising voter confidence." *See* Nat'l Acad. of Scis., Eng'g & Med., *Securing the Vote: Protecting American Democracy* 93 (2018), https://bit.ly/2NHL0Wr. The reason is straightforward: audits "demonstrate the validity of an election outcome and provide an indication of errors in ballot tabulation." *Id.* at 93–94. But the information that audits are based upon must be voter-verified and reliable. Electronic evidence is neither. It "can be altered by compromised or faulty hardware or software." *Id.* at 94. Indeed, when the U.S. Election Assistance Commission tasked the National Institute of Standards and Technology ("NIST") with developing ways to audit DRE-based systems without a paper ballot, NIST could not identify a viable option. Instead, NIST concluded that "[t]he main shortcoming of paperless DREs is in transparency and auditability: they do not provide the capacity for observers, or election officials, to confirm for themselves that the voting equipment worked properly in any particular election." NIST, *Report of the Auditability Working Group* 28 (Jan. 14, 2011), https://www.eac.gov/sites/default/files/eac_assets/1/28/AuditabilityReport_final_January_2011.pdf. "As a result, errors and failures of the equipment may go undetected, which can lead to significant undetected errors in the vote tally." *Id.* Furthermore, even if errors are detected on a given machine, without a valid auditing system it is impossible to separate the "bad" votes from legitimate, correctly recorded votes. *See* Buell & Gay, *supra*, at 40. This inability to differentiate votes

inevitably leads to disenfranchisement: "To choose not to count votes from terminals with errors is to disenfranchise the voters who were directed to those terminals," but "to choose to count the votes is deliberately to include votes that might not be cast as intended." *Id.*

Despite the importance of reliable, paper-based election audits, Shelby County is one of the few jurisdictions in the country to use a *paperless* DRE system. This poses a serious and unnecessary risk to the security of elections in Shelby County. Federal officials tasked with the responsibility to protect our national security have stated that paperless DREs "are at highest risk for security flaws," and "[s]tates should rapidly replace outdated and vulnerable voting systems" with machines that "[a]t a minimum . . . have a voter-verified paper trail." S. Select Comm. on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election* 4, 6 (May 8, 2018), https://www.intelligence.senate.gov/sites/default/files/publications/RussRptInstlmt1.pdf.

Jurisdictions *can* move quickly to replace paperless machines with a more reliable voting system. For example, less than two months before the November 2017 election, Virginia decertified paperless DRE machines—including the Diebold AccuVote-TSx—that 22 of its localities used. *See Cybersecurity of Voting Machines: Joint Hearing Before the Subcomms. on Info. Tech. and Intergovernmental Affairs of the H. Comm. on Oversight and Gov't Reform*, 115th Cong. 23 (2017), https://www.govinfo.gov/content/pkg/CHRG-115hhrg30295/pdf/CHRG-115hhrg30295.pdf (statement of

Edgardo Cortés, Comm'r, Va. Dep't of Elections). Those localities obtained new voting machines in the 59 days before the November 2017 election, and that election "was effectively administered without any reported voting equipment issues." *Id.* at 26. According to the Commissioner of Virginia's Department of Elections, "[t]he transition to paper-based voting systems on a truncated timeline was incredibly successful and significantly increased the security of the election." *Id.* Similarly, in February 2018, Pennsylvania officials issued a directive requiring that all future purchases of voting machines must include the use of voter-verified paper ballots. *See* Media Advisory, *Wolf Administration Directs that New Voting Systems in the Commonwealth Provide Paper Record* (Feb. 9, 2018), https://www.media.pa.gov/Pages/State-Details.aspx?newsid=261.

Shelby County's failure to adopt, at a bare minimum, an auditable voting system to give its voters assurance that their votes are being counted only further underscores the County's imminent and ongoing violations of its voters' rights.

C. As a Result of the Sixth Circuit's Ruling, the Voting Machines At Issue Will Continue To Harm Voters.

C. Asa Result of the Sixth Circuit's Ruling, the Voting Machines At Issue Will Continue To Harm Voters.

In response to all these demonstrated technical errors and vulnerabilities, the Sixth Circuit summarily declared that "plaintiffs have not plausibly shown that there is a substantial risk" of errors or vulnerabilities that would compromise voters' constitutional rights. Pet. App. 9. This case highlights the problem

with the Sixth Circuit's narrow reading of the imminence standard: if experts' conclusions—that the recurring pattern of technical errors and critical vulnerabilities inherent to these voting machines will continue absent corrective action—are insufficient to demonstrate imminence, then the standard imposes an insurmountable bar.

This Court should review the Sixth Circuit's decision, which ignored these recurring technological flaws and instead focused almost exclusively on the errors with some human component of Shelby County's voting system. Critically, the Sixth Circuit also ignored that those past wrongs *themselves* "are evidence bearing on whether there is a real and immediate threat of repeated injury." *O'Shea v. Littleton*, 414 U.S. 488, 496 (1974). And here, those past errors are accompanied by "continuing, present adverse effects," because Shelby County refuses to take any action to remove the voting machines that have proven dysfunctional time and time again. *Id.* As a result, these flawed machines will continue to disenfranchise and dilute voters' rights until the machines are replaced.

The Sixth Circuit's misapprehension of this imminent threat of vote dilution or disenfranchisement has ruinous consequences for the fundamental right to vote. By creating an effectively insurmountable barrier to suits by plaintiffs seeking to preemptively challenge the inevitable harms of deficient voting machines, the decision forecloses intervention by courts to prevent the use of machines that experts have predicted will continue to fail. And it emboldens and

enables states to stand by as their chosen election procedures arbitrarily—yet predictably—impair the fundamental right to vote.

This impact of the Sixth Circuit's ruling is already playing out in Shelby County itself. Although Respondents represented to the Sixth Circuit that new machines would be in place by the November 2020 election, Oral Arg. at 14:20–14:40 (exchange with Gibbons, J.), https://perma.cc/NUN4-DBU4, Shelby County reversed course after the Sixth Circuit issued its opinion and decided *not* to replace the dysfunctional machines in advance of the general election. Rudy Williams, *No New Voting Machines in Shelby County for the November Election*, ABC 24 (Feb. 10, 2020), https://rb.gy/k9e3li. The Sixth Circuit's distortion of Article III's requirement of an actual or imminent harm enables this behavior, and it demands this Court's attention.

II. THE SIXTH CIRCUIT'S DECISION CONFLICTS WITH ELEVENTH CIRCUIT PRECEDENT PERMITTING PLAINTIFFS TO CHALLENGE SIMILAR HARMS TO THEIR VOTING RIGHTS.

The Sixth Circuit's approach would impair courts' ability to intervene to protect the fundamental right to vote. That is more than enough reason for this Court to grant review. But there is more.

The Sixth Circuit's determination that Shelby County's continued deployment of deficient electronic voting machines does not cause an injury to Petitioners runs contrary to Eleventh Circuit precedent,

which has permitted plaintiffs to bring constitutional challenges based on similar—and in some cases, even *identical*—threats of harm in the election context.

Future injuries can establish an imminent risk of harm "if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.'" *Dep't of Commerce v. New York*, 139 S. Ct. 2551, 2565 (2019) (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)). The risk that the AccuVote-TSx DRE machines will continue to malfunction in future elections meets that threshold. But the Sixth Circuit manufactured a higher, unattainable standard, requiring Petitioners to show "Shelby County election officials always make these mistakes" or "government entities ordered the election workers to make any such mistakes." Pet. App. 8. This near-impossible bar is inconsistent with this Court's cases, which "do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013). It is sufficient that the government's failure to replace machines that have consistently resulted in dilution and disenfranchisement has the "predictable effect" of resulting in harm again in the November 2020 election. *Dep't of Commerce*, 139 S. Ct. at 2566.

The Sixth Circuit relied on inapposite cases to heighten the threshold showing of imminent harm, *see* Pet. App. 7–8 (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 105–06 (1983))—an approach that the Eleventh Circuit has already rejected in analogous contexts. In *Florida State Conference of N.A.A.C.P. v. Browning*, 522 F.3d 1153 (11th Cir. 2008), plaintiffs

challenged a law requiring voters to provide a state-issued ID number when registering to vote and requiring election officials to verify the number before registering the voter, arguing that the law provided inadequate procedures to cure errors in the matching process. *Id.* at 1156, 1158. In concluding that plaintiffs established imminent harm, the Eleventh Circuit rejected the imminence requirement articulated in *Lyons*—the same case the Sixth Circuit relied upon—because the threat of harm at issue was the "foreseeable" and "expected result[]" of "unconscious and largely unavoidable human errors in transcription," not based "on conjecture about how individuals will intentionally act in the future." *Id.* at 1163.[6] Likewise, the multiple layers of risks and errors highlighted above stemming from the technological deficiencies with Shelby County's voting system do not suggest that the harm to Petitioners turns on a "highly attenuated chain of possibilities." *Amnesty Int'l*, 568 U.S. at 410. Quite the opposite: as explained above, *any one* of these highly likely errors would lead to dilution or disfranchisement of Shelby County voters. These compounding risks of error, combined with the inability to audit the machines to demonstrate the damage these errors inflict on the fundamental right to vote, pose an obvious risk of imminent harm that courts must be permitted to

---

[6] *See also Williams ex rel. J.W. v. Birmingham Bd. of Educ.*, 904 F.3d 1248, 1265, 1269 (11th Cir. 2018) (distinguishing *Lyons* where plaintiffs "could expect to be future victims of more of the same harms they had alleged because they faced those harms due to circumstances they could not change"); *Honig v. Doe*, 484 U.S. 305, 320 (1988) (distinguishing *Lyons* where plaintiff is unable to control his behavior).

address. Because of these purely technical errors and "largely unavoidable human errors," the risk of harm is sufficiently imminent, even if the mistakes "cannot be identified in advance" with the literal certainty that the Sixth Circuit demanded. *Browning*, 522 F.3d at 1164.

A recent district court case from within the Eleventh Circuit demonstrates this direct conflict between Sixth and Eleventh Circuit precedent on plaintiffs' ability to seek a court's relief to remedy technological deficiencies in their state's voting system. In *Curling v. Raffensperger*, plaintiffs argued that Georgia's use of a paperless DRE system—a system that relies on the exact same voting machines used in Shelby County—constitutionally infringed on their right to vote, because such an election system has been proven unreliable and susceptible to hacking, and the machines do not leave an auditable paper trail. 403 F. Supp. 3d 1311, 1318–19 (N.D. Ga. 2019). The court agreed that plaintiffs had suffered a cognizable injury because, under Eleventh Circuit precedent, plaintiffs had "alleged that Defendants were aware of serious security breaches in the DRE voting system and failed to take adequate steps to address those breaches." *Id.* at 1344–45. On the same material facts, the Sixth Circuit has reached the opposite result. This stark conflict highlights the need for this Court's review.[7]

In *Curling*, the court relied on three core categories of factual allegations to reach its conclusion that

---

[7] The Supreme Court of Texas has also allowed plaintiffs to challenge the certification and use of a paperless DRE system. *Andrade v. NAACP of Austin*, 345 S.W.3d 1, 9–10 (Tex. 2011).

plaintiffs had suffered a non-speculative injury. Those same three categories of allegations are present in equal, if not greater, force in this case.

First, evidence from election security experts bolstered the *Curling* plaintiffs' claims as non-speculative. As the court explained, "national security experts and cybersecurity experts at the highest levels of our nation's government and institutions have weighed in on the specific issue of DRE systems in upcoming elections and found them to be highly vulnerable to interference, particularly in the absence of any paper ballot audit trail." *Curling*, 403 F. Supp. 3d at 1340. Another expert showed how a "contaminated memory card's malware" could "change[] the actual votes cast between candidates" during "a live demonstration in Court with a Diebold DRE using the same type of equipment and software as that used in Georgia" (and in Shelby County). *Id.* at 1319–20. Perhaps most alarmingly, the vote manipulation in the demonstration left "no means of detection," *id.*, suggesting that election officials would have no way of knowing if the same thing happened in an actual election. Here, too, Petitioners and independents experts have offered myriad evidence that Shelby County's election system is vulnerable to attack. Because Shelby County uses the same voting machines at issue in *Curling*, any evidence offered by cybersecurity experts in that case about the vulnerabilities of those machines applies equally to Shelby County's machines. In addition, at a recent conference, computer hackers with only legally and publicly available information were able to breach a range of actual voting machines, including the AccuVote-TSx DRE machine

used in Shelby County. *See* Matt Blaze et al., *DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure* 9–10 (2017), https://bit.ly/2oQb5dA.

Second, the harm that the *Curling* plaintiffs alleged was not speculative because at least some manifestations of that harm had already occurred. *See Curling*, 403 F. Supp. 3d at 1340. As discussed above, Petitioners and other voters in Shelby County have already experienced injuries resulting from the technological deficiencies with the county's voting machines. There have been countless reports over more than a decade of AccuVote-TSx machines in Shelby County flipping votes or malfunctioning in other ways. *See supra* Part I.A. In light of these errors, Petitioners have shown that they reasonably cannot trust that their vote in a Shelby County election will be accurately recorded and counted, nor that the County's election results accurately represent the will of *all* the voters. The very fact that citizens are forced to participate in an election system that continues to dilute votes is an injury in and of itself.

Third, the *Curling* plaintiffs alleged that harm would recur because the defendants knew of the voting system's inadequacies and failed to take adequate corrective or preventative measures. In *Curling*, the court found that plaintiffs "plausibly allege[d] a threat in upcoming elections . . . that would jeopardize their votes and the voting system at large" because, "[d]espite being aware of election system and data cybersecurity threats and vulnerabilities identified by national authorities . . . Defendants allegedly have

not taken steps to secure the DRE system from such attacks." *Id.* at 1341. Similarly, Respondents here have long known about the AccuVote-TSx DRE's inadequacies and have failed to take preventative measures. Even the current Secretary of State, a Respondent in this lawsuit, has admitted that "nearly every election cycle in the county in recent memory has been plagued by a myriad of errors and complaints of wrongdoing." Compl. Ex. A at 1, Dist. Ct. Doc. 104-6. Notwithstanding these known deficiencies, election officials continue deploying the AccuVote-TSx DRE machines: Respondents went so far as to concede during oral argument in the Sixth Circuit that the same dysfunctional machines would be used in the March 3, 2020 Tennessee primary election, Oral Arg. at 13:14–14:20, https://perma.cc/NUN4-DBU4, and they have since decided not to replace the machines for the November 2020 election, *see* Williams, *supra*.

The Sixth Circuit's basis for distinguishing *Curling* is untenable. The court reasoned that the fact that the DRE election system in Georgia—a system that relies on the exact same machines used in Shelby County—was breached on multiple occasions "does not translate into an imminent risk that individuals will hack the voting machines in Shelby County." Pet. App. 12.

But as *amici* argued before the Sixth Circuit, voting systems in Tennessee, and specifically in Shelby County, *have* been the target of malicious hacking and have been prone to other serious security breaches. In 2018, for example, computers from sixty-five foreign countries attacked the election commission server in

Knox County, Tennessee, shutting down the website for several hours on the night that primary election results were being reported. Jennifer Barrie et al., Tenn. Advisory Comm'n on Intergovernmental Relations, *Tennessee's Election Security: A Staff Update* 4 (2018), https://bit.ly/33evt6Y. In 2006, a "critical security breach" occurred during a Shelby County election when the Diebold central tabulator was plugged into the County network and unauthorized software was installed. Green et al., *supra*, at 75–76.

Furthermore, the Department of Homeland Security and Federal Bureau of Investigation issued a joint intelligence bulletin confirming that Russian hacking activities targeted the election systems in all fifty U.S. states, including Tennessee, in the 2016 election. *See* Sean Gallagher, *DHS, FBI Say Election Systems in All 50 States Were Targeted in 2016*, Ars Technica (Apr. 10, 2019), https://bit.ly/33kaZcY. The U.S. law enforcement agencies described these efforts as "methodical reconnaissance" in which the Russian hackers "prob[ed] for potential vulnerabilities in election systems" at "both the state and local level." *Id.* Though the extent of the Russian hackers' efforts in each state has not been publicly disclosed, it is clear that Tennessee's voting system was not spared in Russian cyber-attackers' attempts to manipulate the 2016 U.S. election. *See Curling*, 403 F. Supp. 3d at 1340 (noting that defendants' arguments "completely ignore the reality faced by election officials across the country underscored by Plaintiffs' allegations that electronic voting systems are under unceasing attack").

The Sixth Circuit also failed to recognize that the technological deficiencies that make paperless DRE machines susceptible to vote manipulation in Georgia also make those machines susceptible to vote manipulation in Tennessee—or wherever they are deployed. According to the Sixth Circuit, the fact that a DRE election system relying on AccuVote-TSx machines was breached twice in Georgia showed an "imminent harm somewhere in Georgia" but not in Shelby County. But there is nothing inherent about Georgia—or the types of hackers that might target Georgian elections—that makes Accu-Vote-TSx DREs vulnerable to vote manipulation only in Georgia. Indeed, the Sixth Circuit overlooked that the DRE election system in Georgia was hacked "by cybersecurity experts who reported the system's vulnerabilities to state authorities, *as opposed to someone with nefarious purposes*." *Curling*, 403 F. Supp. 3d at 1340 (emphasis added). That is to say, computer scientists set about—and succeeded in—demonstrating that the DRE election system *could be hacked*, and that was sufficient to prove that the Georgia plaintiffs "plausibly allege[d] a threat in up-coming elections of a future hacking event that would jeopardize their votes and the voting system at large." *Id.* at 1341. By the Sixth Circuit's logic, when experts demonstrate a voting system to be inherently unreliable, that system is constitutionally deficient for voters who happen to live in the jurisdiction where the experts conducted their work, but it raises no constitutional problems for voters in other parts of the country who use *identical* voting technology. Voting machines' technological vulnerabilities do not observe such neat jurisdictional lines. The problem here is not with paperless DRE

machines *in Georgia*, but rather with paperless DRE machines, full stop.

The Supreme Court must resolve this circuit split to allow voters to seek redress from a court when deficient voting technology threatens their fundamental right to have their votes properly recorded and counted.

There are 13 references to Georgia in this document.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

Courtney Hostetler
Ronald Fein
John Bonifaz
Ben Clements
FREE SPEECH FOR PEOPLE
1320 Centre St. #405
Newton, MA 02459
(617) 249-3015

John D. Graubert
Counsel of Record
Megan C. Keenan
Ryan Miller
Jeremy Patashnik
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
jgraubert@cov.com
(202) 662-6000

July 22, 2020

Counsel for Amici Curiae