19-6142

In the United States Court of Appeals for the Sixth Circuit

SHELBY ADVOCATES FOR VALID ELECTIONS, *et al.*,
Plaintiff-Appellants,

v.

TRE HARGETT, *et al.*,
Defendant-Appellees

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE AT MEMPHIS
2:18-CV-02706-TLP-DKV

BRIEF OF THE NATIONAL ELECTION DEFENSE COALITION, U.S. TECHNOLOGY POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING MACHINERY, AND OTHER INDIVIDUAL ELECTION SECURITY EXPERTS* AS AMICI CURIAE IN SUPPORT OF PLAINTIFF-APPELLANTS AND REVERSAL

Megan C. Keenan
Counsel of Record
John D. Graubert
Ryan Miller†
Jeremy Patashnik†
COVINGTON & BURLING LLP
850 Tenth St. NW
Washington, D.C. 20001
(202) 662-6000

Counsel for NEDC and Individual Amici Curiae

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

Andrew Grosso
ANDREW GROSSO & ASSOCIATES
1101 Thirtieth St. NW
Suite 500
Washington, D.C. 20007
(202) 298-6500

Counsel for U.S. Technology Policy Committee of the Association for Computing Machinery

November 7, 2019

* A full list of *amici* appears in the brief's Statement of Interest.

† Law Clerk

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 19-6142 Case Name: SAVE, et al. v. Hargett, et al.

Name of counsel: Megan C. Keenan

Pursuant to 6th Cir. R. 26.1, National Election Defense Coalition
Name of Party
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

N/A

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

N/A

CERTIFICATE OF SERVICE

I certify that on November 7, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Megan C. Keenan

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 19-6142 Case Name: SAVE, et al. v. Hargett, et al.

Name of counsel: Andrew Grosso

Pursuant to 6th Cir. R. 26.1, U.S. Technology Policy Committee of the Association for Computing Machinery
Name of Party

makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

N/A

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

N/A

CERTIFICATE OF SERVICE

I certify that on November 7, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/Megan C. Keenan
Andrew Grosso

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

STATEMENT OF INTEREST 1

INTRODUCTION 3

SUMMARY OF ARGUMENT 5

ARGUMENT 6

I. Shelby County's Voting System Arbitrarily Dilutes Voting Power. 8

II. Shelby County's Voting System Arbitrarily Frustrates Voters' Abilities to Elect Their Preferred Candidate. 15

III. Shelby County's Voting System Has Known Defects that Make It Susceptible to Manipulation and Attack. 17

IV. Shelby County's Voting System Cannot Be Verifiably Audited to Address and Correct Errors and Vulnerabilities in Future Elections. 23

CONCLUSION 27

TABLE OF AUTHORITIES

Page(s)

Cases

Baker v. Carr, 369 U.S. 186 (1962) 8, 17

Black v. McGuffage, 209 F. Supp. 2d 889 (N.D. Ill. 2002) 7

Bush v. Gore, 531 U.S. 98 (2000) 5, 8

Citizens in Charge v. Husted, Nos. C2-08-1014, C2-10-095, 2011 WL 3652701 (S.D. Ohio Aug. 19, 2011) 7

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

Ex parte Siebold, 100 U.S. 371 (1879) 24

FEC v. Akins, 524 U.S. 11 (1998) 6

Gray v. Sanders, 372 U.S. 368 (1963) 6, 8

Hunter v. Hamilton Cty. Bd. of Elections, 635 F.3d 219 (6th Cir. 2011) 8, 24

League of Women Voters of Ohio v. Brunner, 548 F.3d 463 (6th Cir. 2008) 8, 9

Reynolds v. Sims, 377 U.S. 533 (1964) ..... passim

Sandusky Cty. Democratic Party v. Blackwell, 387 F.3d 565 (6th Cir. 2004) 6, 14, 15, 24

Stewart v. Blackwell, 444 F.3d 843 (6th Cir. 2006), *vacated as moot* (July 21, 2006), *superseded*, 473 F.3d 693 (6th Cir. 2007) ..... passim

United States v. Classic, 313 U.S. 299 (1941) 14, 15

United States v. Netyksho, 1:18-cr-00215-ABJ (D.D.C. July 13, 2018) 18

Yick Wo v. Hopkins, 118 U.S. 356 (1886) 4

Other Authorities

Calif. Sec'y of State, Withdrawal of Approval (Oct. 25, 2007), https://bit.ly/34tJEFp 14, 29

Carol Chumney et al., *Voting on Thin Ice* (2017), https://bit.ly/2WHceAr 11, 12, 20

Danielle Root et al., *Election Security in All 50 States: Defending America's Elections* (2018), https://ampr.gs/2pJwZ2m.....29

Duncan Buell & Gregory Gay, *Is Technology the Answer? Software Quality Issues in Electronic Voting Systems* (2019), https://bit.ly/36zQBXy..... 17, 31

Edgardo Cortes, Commissioner of Virginia Dep't of Elections Testimony to Subcomms. of U.S. House Comm. on Oversight and Gov't Reform (Nov. 29, 2017), https://bit.ly/32antmc..... 15, 21

Election Science Inst., *DRE Analysis for May 2006 Primary, Cuyahoga County, Ohio* (2006), https://bit.ly/2CdsUGw 14

Harry A. Green et al., *Trust But Verify: Increasing Voter Confidence in Election Results*, Tennessee Advisory Commission on Intergovernmental Relations (2007), https://bit.ly/2NgzJO0 3

Jennifer Barrie & David Lewis, *Tennessee's Election Security: A Staff Update*, Tennessee Advisory Commission on Intergovernmental Relations (2018), https://bit.ly/33evt6Y 24

Joseph A. Calandrino et al., *Source Code Review of the Diebold Voting System* (2007), https://bit.ly/34AXdCY 14, 27

Lawrence Norden & Christopher Famighetti, Brennan Ctr. for Justice, *America's Voting Machines at Risk* (2015), https://bit.ly/36ysb0x 21

Lawrence Norden, *Voting System Failures: A Database Solution* (2010), https://bit.ly/2JTEivk 13

Mark Mazzetti & Katie Benner, *12 Russian Agents Indicted in Mueller Investigation*, N.Y. Times (July 13, 2018), https://nyti.ms/2Clcn37 23

Matt Blaze et al., *DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure* (2017), https://bit.ly/2oQb5dA 25, 26

NIST, *Report of the Auditability Working Group* (Jan. 14, 2011), https://bit.ly/36zvip5 33

Patrick McDaniel et al., *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing* (2007), https://bit.ly/2K0FGfY 27

Sean Gallagher, *DHS, FBI Say Election Systems in All 50 States Were Targeted in 2016*, Ars Technica (Apr. 10, 2019), https://bit.ly/33kaZcY 24

Shelby County RFQ # 15-008-10 Consultant Services Replacement of Election System Management Software, https://bit.ly/2NHWGZ4.....4

The National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* (2018), https://www.nap.edu/read/25120/chapter/1..... 32, 33

WMC Action News 5, *Stylus Added to Voting Machine to Help Avoid Vote Flipping* (Nov. 1, 2016, 3:26 PM), https://bit.ly/34tQtH1 20

STATEMENT OF INTEREST

All parties have consented to the filing of this brief. 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. *See* Fed. R. App. 29(a)(4)(E).

Amici curiae are: (1) the National Election Defense Coalition ("NEDC") and individual election security experts; and (2) the U.S. Technology Policy Committee ("USTPC") of the Association for Computing Machinery ("ACM").

The NEDC is a national network of recognized experts in cybersecurity and elections administration, bipartisan policymakers, and concerned citizens. The NEDC works to build a bipartisan consensus on the need for reform, while building a comprehensive, cost-effective plan to secure the vote in coming elections.

ACM, a non-profit and non-lobbying 501(c)(3) organization, is the nation's and the world's largest and longest-established society of individual professionals engaged in all aspects of computing. USTPC serves as the focal point for ACM's interaction with all branches of the U.S. government, the computing community, and the public on policy matters related to information technology. Its members include election security experts.

Amici are also the following individuals with expertise in the security of electronic voting systems:[1]

Duncan A. Buell, Professor, Department of Computer Science and Engineering and NCR Chair of Computer Science and Engineering, University of South Carolina.

Richard DeMillo, Professor, Charlotte B. and Roger C. Warren Chair of Computing, and Director of the Center for 21st Century Universities ("C21U"), Georgia Institute of Technology.

Bruce Schneier, Adjunct Lecturer in Public Policy, Harvard Kennedy School, and Fellow at the Berkman Klein Center for Internet & Society, Harvard University.

Eugene H. Spafford, Professor of Computer Science, Purdue University, and Executive Director Emeritus of Center for Education and Research in Information Assurance and Security, Purdue University.

Philip B. Stark, Associate Dean, Division of Mathematical and Physical Sciences, and Professor of Statistics, University of California.

[1] Institutional affiliations are provided for identification purposes only and do not constitute or reflect institutional endorsement.

INTRODUCTION

In Shelby County, registered voters cast their ballots knowing that, through no fault of their own, their ballots might not be counted or afforded the same weight as other votes. Yet the district court determined that Plaintiffs—Shelby County voters and an organization representing Shelby County voters—had suffered no injury from this violation of their voting rights. In doing so, the court misunderstood the nature of Plaintiffs' injuries and underestimated what election and national security experts recognize as serious flaws in the Shelby County voting system.

In every election cycle since Shelby County purchased the Diebold AccuVote-TSx direct-recording electronic election system ("AccuVote-TSx DRE") in 2006, thousands of voters have seen their votes miscounted or been given the wrong ballot. Voters report having had their votes flipped, their data manipulated, their registration statuses stripped, and their personal records sold and publicly exposed. Pls.' Second Am. Compl., ECF 104, ¶¶ 132, 137, 149, 151, 152, 154, 155, 169, 173, 174, 176, 178, 233, 241, 246; *see also* Harry A. Green et al., Tenn. Advisory Comm'n on Intergovernmental Relations, *Trust But Verify: Increasing Voter Confidence in Election Results* 21–22, 25–26, 36 (2007), https://bit.ly/2NgzJO0 [hereinafter Green et al., *Trust But Verify*] (detailing the system's vulnerabilities and errors in Shelby County and elsewhere in the country). These problems will only worsen with time, especially because the AccuVote-TSx

is no longer manufactured and its vendor no longer services its software. Pls.' Second Am. Compl., ECF 104, ¶ 84. 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 County RFQ # 15-008-10 Consultant Services Replacement of Election System Management Software, https://bit.ly/2NHWGZ4. And there is no way to verify that the machines correctly counted votes and correctly recorded voter preference. Pls.' Second Am. Compl., ECF 104, ¶ 87.

These deficiencies result in serious infringements of Shelby County voters' "fundamental" right to vote, a right that has long been zealously guarded by the courts as "preservative of all rights." *See Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886). This right is not limited to a person's ability to submit a ballot: "the right of suffrage can be denied by a debasement or dilution of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise." *Reynolds v. Sims*, 377 U.S. 533, 555 (1964).

Shelby County cannot infringe on its voters' rights to vote by deploying deficient technology and remain unaccountable for future violations caused by the same technology. *See Stewart v. Blackwell*, 444 F.3d 843, 876–77 (6th Cir. 2006), *vacated as moot*, (July 21, 2006), *superseded*, 473 F.3d 693 (6th Cir. 2007) ("Technology, as a method or means to dilute voting strength, is no less a violation

than any other invidious method."). The harm suffered by Shelby County voters is not less real because a faulty voting system is at the root of the injury. *See id.* (holding that the election technologies being challenged "fail[ed] to satisfy 'rudimentary requirements of equal protection and fundamental fairness' and that . . . the plaintiffs established a violation of the Equal Protection Clause" (quoting *Bush v. Gore*, 531 U.S. 98, 109 (2000) (*per curiam*))); *Curling v. Kemp*, 334 F. Supp. 3d 1303, 1316 (N.D. Ga. 2018) (explaining that courts have found plaintiffs have suffered an injury where plaintiffs have alleged vote miscounting due to "certain voting technology"). Plaintiffs have suffered a definite and serious injury in fact as a result of Shelby County's many impingements on their voting rights.

SUMMARY OF ARGUMENT

Shelby County's electronic voting system—the paperless AccuVote-TSx DRE—imparts real and imminent injury to the federally protected right to vote. The AccuVote-TSx DRE system arbitrarily dilutes voting power by undercounting certain votes, providing some voters with the wrong ballots, and arbitrarily assigning votes to incorrect candidates, thereby empowering some voters at the expense of others. In addition, known defects in the voting system make it uniquely susceptible to undetectable foreign and domestic interference. Cybersecurity and elections experts of all political orientations have warned of the dangers posed by such vulnerabilities. The harms wrought by these known defects are compounded by the

fact that AccuVote-TSx DRE machines offer no verifiable process for auditing election results. For all of these reasons, this system imparts a real and serious injury to the residents of Shelby County—including Plaintiffs—by interfering with their voting rights. The Court should reverse the district court's dismissal of Plaintiffs' Complaint.

ARGUMENT

Plaintiffs have demonstrated that Shelby County's reliance on the defective AccuVote-TSx DRE voting system has violated, and will continue to violate, their core voting rights. As such, Shelby County's voting system imparts real and imminent injury to the federally protected right to vote.

Plaintiffs' claims of the violations of citizens' voting rights "present a justiciable controversy subject to adjudication by federal courts." *See Reynolds*, 377 U.S. at 556. And any voter may bring a lawsuit "where large numbers of voters suffer interference with voting rights conferred by law." *FEC v. Akins*, 524 U.S. 11, 24 (1998); *see also Gray v. Sanders*, 372 U.S. 368, 375 (1963); *Sandusky Cty. Democratic Party v. Blackwell*, 387 F.3d 565, 574 (6th Cir. 2004) (finding sufficient injury in fact although plaintiffs had "not identified specific voters" whose rights would be infringed on Election Day). Indeed, courts have described the ability to maintain a suit as "broad" where the challenge is to an electoral system that advantages some voters over others. *See Citizens in Charge v. Husted*, Nos. C2-08-

1014, C2-10-095, 2011 WL 3652701, at *3 (S.D. Ohio Aug. 19, 2011); *see also Black v. McGuffage*, 209 F. Supp. 2d 889, 895 (N.D. Ill. 2002) (finding "probabilistic" injury was sufficient to maintain suit when the harm asserted was "not the State's failure to count any one person's vote, but the higher probability of that vote not being counted as a result of the voting systems used").

Plaintiffs' claims in this case implicate their core voting rights in at least four ways:

First, Shelby County's error-prone voting system dilutes its citizens' votes by, according to voters and State and local officials, arbitrarily assigning votes to the wrong candidates, deleting votes entirely, undercounting and miscounting votes, and providing voters with the wrong ballots.

Second, Shelby County's voting system arbitrarily frustrates voters' abilities to elect their preferred candidates by reportedly flipping votes.

Third, with the growing threat of malicious election interference, Shelby County has chosen to use a voting system that is particularly susceptible to sophisticated, high-tech ballot box tampering.

Fourth, Shelby County's paperless system cannot be audited, which severely limits the County's ability to detect malicious tampering and inadvertent error. This also undermines voter confidence in Shelby County and virtually ensures that Shelby County's flawed voting system will continue to injure Plaintiffs in future elections.

Plaintiffs have suffered real, certain, and imminent harm from this inherently defective voting system. Therefore, the Court should reverse the district court's dismissal of Plaintiffs' Complaint.

I. Shelby County's Voting System Arbitrarily Dilutes Voting Power.

The right to vote is about more than just access to the polls. Both this Court and the Supreme Court have held that states cannot impair the right to vote by arbitrarily diluting votes. *See Baker v. Carr*, 369 U.S. 186, 208 (1962); *see also Reynolds*, 377 U.S. at 558 (the Constitution's "conception of political equality" requires that votes be afforded equal weight (quoting *Gray*, 372 U.S. at 381)); *Hunter v. Hamilton Cty. Bd. of Elections*, 635 F.3d 219, 234–35 (6th Cir. 2011) ("[W]e have held that [t]he right to vote includes the right to have one's vote counted on equal terms with others. . . . We are therefore guided in our analysis by the important requirement that state actions in election processes must not result in arbitrary and disparate treatment of votes." (internal citations and quotation marks omitted)); *League of Women Voters of Ohio v. Brunner*, 548 F.3d 463, 476–78 (6th Cir. 2008) ("At a minimum . . . equal protection requires 'nonarbitrary treatment of voters.'" (quoting *Bush*, 531 U.S. at 105)). "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." *Bush*, 531 U.S. at 104–05; *League of Women*

Voters of Ohio, 548 F.3d at 476. Errors that cause vote dilution "present a justiciable controversy subject to adjudication by federal courts." *Reynolds*, 377 U.S. at 556.

The AccuVote-TSx DRE has been in use in Tennessee for more than thirteen years, and since the beginning it has been plagued with errors that have led to vote dilution. Voters have been subject to elections in which results were certified even where the numbers reported did not match the vote-tally tape. *See* Pls.' Second Am. Compl., ECF 104, ¶ 154. Some of these errors can be attributed to the insecure memory cards used by the AccuVote-TSx DRE machine. In one instance, thirty memory cards were uploaded in a precinct with only nine machines; twenty-one of these memory cards were uploaded before polls closed. Pls.' Second Am. Compl., ECF 104, ¶ 149; Carol Chumney et al., *Voting on Thin Ice* 40–41 (2017), https://bit.ly/2WHceAr [hereinafter Chumney et al., *Voting on Thin Ice*]. In 2015, hundreds of votes were uploaded between eleven and twenty-two days after the polls closed—and this delayed upload only took place after a citizen photographed a poll tape, identified discrepancies between the tape and reported vote totals, and brought it to a candidate's attention. Pls.' Second Am. Compl., ECF 104, ¶¶ 152, 155.[2] Shelby County Election Commissioner Norma Lester (a Defendant-Appellee) has

[2] Because Shelby County election officials for a number of years failed to conduct a simple and state-law mandated audit—checking to see if precinct tally poll tapes matched tabulated results—the problem of under- or over-voting likely has been even more widespread than reported. Tenn. Code Ann. § 2-8-104; Pls.' Second Am. Compl., ECF 104, ¶¶ 157, 187.

admitted that election officials could not reconcile the number of voters who signed in to vote with the tally numbers recorded by the machines used during early voting. Pls.' Ex. L, ECF 104-18 (stating that "every night during early voting," the Commission "couldn't get the totals to balance," and noting: "I worry about what they do to make them balance. There has [*sic*] been rumors that ballots have been backed out"). In other words, there were either more votes cast than there were voters—which would mean that legitimate votes were diluted against those extra votes—or there were fewer votes counted than there were voters—which would mean that some votes were not counted at all.

In addition, in thousands of instances in recent County elections, documented below, voting machines have displayed the wrong ballot to voters. Some voters in Shelby County have been given ballots that contain contests they were not eligible to vote in, while other voters were given ballots that did not contain contests they *were* eligible to vote in. *See* Chumney et al., *Voting on Thin Ice* 14–15. In an August 2012 local election, for example, a voter reported that two school board districts appeared on her ballot, even though she was only eligible to vote in one. *Id.* And in a 2008 municipal election, entire ballots failed to load at certain precincts, resulting in some voters using paper ballots and others simply not being able to vote in that election. *See* Lawrence Norden, *Voting System Failures: A Database Solution*, app. B, at 87–88 (2010), https://bit.ly/2JTEivk. This problem has arisen in

subsequent elections as well. Pls.' Second Am. Compl., ECF 104, ¶¶ 152, 155. The result of this systemic deficiency in the County's elections process is that the votes of some Shelby County voters are worth less than those of other Shelby County voters.

The vulnerabilities in the AccuVote-TSx DRE are well known nationwide. In 2005, California refused to certify the AccuVote-TSx DRE with its optional printer after a mock election found the machines to have a 10% error rate. Green et al., *Trust But Verify* at 36. Two years later, the California Secretary of State commissioned experts at the University of California, Berkeley, to conduct an in-depth expert analysis of the Diebold voting system, including the AccuVote-TSx DRE (which, without printer attachment, was at the time still certified in California). *See* Joseph A. Calandrino et al., *Source Code Review of the Diebold Voting System* (2007), https://bit.ly/34AXdCY [hereinafter Calandrino et al., *Source Code Review*]. Due to the myriad vulnerabilities in the system exposed during the evaluation, California decertified the AccuVote-TSx DRE. *See* Calif. Sec'y of State, Withdrawal of Approval (Oct. 25, 2007), https://bit.ly/34tJEFp [hereinafter Calif. Sec'y of State, Withdrawal of Approval]. In 2006, the Cuyahoga County Board of Commissioners commissioned the Election Science Institute ("ESI") to assess the AccuVote-TSx system, then in use in Cuyahoga County, Ohio. After "exhaustive research," the ESI found that the machine had four sources of vote totals, none of

which agreed with each other. ESI, *DRE Analysis for May 2006 Primary, Cuyahoga County, Ohio* 2 (2006), https://bit.ly/2CdsUGw. And Virginia has decertified its DRE systems, including the AccuVote-TSx, due to vulnerabilities that render election results unreliable. *See* Edgardo Cortes, Comm'r of Va. Dep't of Elections, Testimony to Subcomms. of U.S. House Comm. on Oversight and Gov't Reform 3 (Oct. 24, 2017), https://bit.ly/32antmc.

Governmental authorities in Tennessee and in Shelby County are well aware of the long-standing and recurring nature of the AccuVote-TSx DRE's vulnerabilities. A 2007 study prepared for the Tennessee Advisory Commission on Intergovernmental Relations identified numerous issues with the AccuVote-TSx DRE, both in Tennessee and nationwide. Green et al., *Trust But Verify* at 21–22, 36. The *Trust But Verify* report concluded that AccuVote-TSx DRE machines are especially susceptible to vote manipulation through intentional misconduct, poll-worker error, and outside hacking. *See infra* Section III. And in a 2012 letter to the Shelby County Election Commission Administration, Tennessee's Secretary of State (and Defendant-Appellee) Tre Hargett requested an audit of Shelby County's elections because "nearly every election cycle in the county in recent memory has been plagued by a myriad of errors and complaints of wrongdoing." Pls.' Ex. A at 1, ECF 104-6. Hargett specifically expressed concern that "over one thousand voters [in Shelby County] had been given the wrong ballot during early voting." *Id.*

Vote undercounting, miscounting, and ballot misassignment have resulted in the arbitrary dilution of votes within Shelby County itself. In addition, the problems that plague Shelby County voters have resulted in the dilution of Shelby County votes relative to Tennessee counties that use more reliable means of voting, such as hand-marked paper ballots counted by optical scanners,[3] and which therefore are not subject to many of the same failures associated with the deficient AccuVote-TSx DRE technology. *See Stewart*, 444 F.3d at 861 (concluding "voters facing deficient technology approach the ballot in a position unequal from the portion of the electorate using adequate technology"). Finally, Plaintiffs have shown that they reasonably cannot trust that any Shelby County election is accurate, or that the County's election results accurately represent the will of *all* the people. The very fact that citizens are forced to participate in an election system that continues to an unacceptable degree of probability to dilute votes is an injury in and of itself.

Vote dilution will almost certainly recur in future elections for as long as Shelby County relies on a DRE such as the AccuVote-TSx. As two election security experts explained, there is an "inherent problem" in trying to detect individual instances of software error in DRE voting systems, because "there is no way to

[3] Counties that use more reliable methods of voting also will, pursuant to Tennessee law, be robustly audited. *See* Tenn. Code Ann. § 2-20-103 (requiring counties that use optical scanners to conduct public automatic audits and a hand count in the case of variances of more than 1% between the automatic audit and the unofficial election results). The AccuVote-TSx DRE, however, is unable to reliably detect and correct inaccurate vote counts through the conduction of post-election audits.

determine [the] ground truth of the results and virtually no way to test the software at scale[.]" Duncan Buell & Gregory Gay, *Is Technology the Answer? Software Quality Issues in Electronic Voting Systems* 39 (2019), https://bit.ly/36zQBXy [hereinafter Buell & Gay, *Is Technology the Answer?*]. Those experts concluded that "each software fault arguably causes *great damage* to the users and environment of the system by falsely amplifying, misrepresenting, or disenfranchising their vote." *Id*. at 40 (emphasis in original).

The AccuVote-TSx DRE balloting errors are no different from the voting rights injuries that courts routinely redress. It is well-established that the right to vote may not be diluted "by alteration of ballots or improper counting of the ballots." *Stewart*, 444 F.3d at 856–57 (citing *United States v. Classic*, 313 U.S. 299, 315 (1941)). As this Court explained in *Stewart*, "voters facing deficient technology" have suffered an injury in fact because they "approach the ballot in a position unequal from the portion of the electorate using adequate technology." *Id.* at 861. And it is no answer to say that Plaintiffs may or may not be able to prove that their particular votes will be miscounted or denied due to a ballot mistake, because "by their nature, mistakes cannot be specifically identified in advance." *Sandusky Cty. Democratic Party*, 387 F.3d at 574. When a voter shows, however, that "[i]t is inevitable . . . that there will be such mistakes," that voter has suffered a "real and imminent" injury. *Id.* In short, Plaintiffs' injury is exactly the type that this Court

has held gives rise to a cognizable claim. *Id.*; *see also Curling*, 334 F. Supp. 3d at 1319–20 (finding that plaintiffs suffered an injury in fact as required to challenge the AccuVote-TSx being used in Georgia).

II. Shelby County's Voting System Arbitrarily Frustrates Voters' Abilities to Elect Their Preferred Candidate.

Individuals do not truly have the right to vote if they cannot be confident that their ballots will not be changed: "The right to vote freely *for the candidate of one's choice* is of the essence of a democratic society." *Reynolds*, 377 U.S. at 555 (emphasis added). The alteration of ballots dilutes votes and violates the rights of voters. *See Stewart*, 444 F.3d at 856–57 (citing *Classic*, 313 U.S. at 315). Alterations caused by technological errors in a voting system are as unconstitutional as other forms of ballot alteration and give rise to a cognizable claim. *Id.* at 871, 876–77; *Curling*, 334 F. Supp. 3d at 1316. Shelby County's error-prone voting system arbitrarily frustrates voter choices and thus has inflicted a real and definite injury upon the voters of Shelby County.

It is well-documented that Shelby County's AccuVote-TSx terminals frequently assign votes to the wrong candidates. 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 voting machine "defaulted or bounced up to the first person on the ballot." Chumney et al., *Voting on Thin Ice* 40–41. During the 2016 federal elections, it was also reported

that the 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, as well as additional votes for the second candidate not being selected at all. WMC Action News 5, *Stylus Added to Voting Machine to Help Avoid Vote Flipping* (Nov. 1, 2016), https://bit.ly/34tQtH1. Shelby County's own Election Commissioner, Norma Lester, expressed concern about the AccuVote-TSx machines being prone to vote flipping in the 2016 national presidential election, citing "numerous occasions when selecting Hillary the vote flips to Trump and when selecting Trump his [vote] is totally removed from the ballot." Chumney et al., *Voting on Thin Ice* 41. Though the Shelby County Election Commission attempted to fix this problem simply by advising voters to use a stylus on these touchscreens, vote-flipping problems have continued to plague voters in more recent elections. Pls.' Ex. S at 2, ECF 104-24. In the 2018 election, one voter reported six instances of vote flipping when she tried to cast her ballot using the AccuVote-TSx DRE. *Id.*[4] These well-documented instances of vote-flipping inflict a real and definite injury by frustrating the voting

[4] The AccuVote-TSx has caused vote flipping in Virginia as well. In 2014, 26 AccuVote-TSx machines in Virginia Beach repeatedly registered a different candidate than the one selected by the voter, due to degrading glue in the aging machines. Lawrence Norden & Christopher Famighetti, Brennan Ctr. for Justice, *America's Voting Machines at Risk* 13 (2015), https://bit.ly/36ysb0x; Edgardo Cortes, Presentation to Senate Finance Committee, Virginia Department of Elections 5 (2015), https://bit.ly/2NF6q6x.

rights of Shelby County voters, and these errors will continue if corrective action is not taken.

III. Shelby County's Voting System Has Known Defects that Make It Susceptible to Manipulation and Attack.

State action cannot allow the votes in the ballot box to be intentionally altered. *See Baker*, 369 U.S. at 208. Yet Shelby County has deliberately chosen to deploy a voting system that is especially susceptible to manipulation and attack. As a result, Shelby County's voting system is at undue risk of ballot box tampering from wrongdoers here and abroad. This acute vulnerability to election tampering represents still another real and definite injury suffered by Plaintiffs.

This is not the first time that voters have sought judicial intervention to guard their votes against interference. Courts have recognized that it is not enough for states merely to refrain from stuffing the ballot box. *See Stewart*, 444 F.3d at 856–57 ("Dilution of the right to vote may not be accomplished by stuffing the ballot-boxes. Nor may the right to vote be diluted by alteration of ballots or improper counting of ballots." (citations omitted)). Rather, voters may maintain a suit based on allegations that a DRE voting system is susceptible to malicious hacking or manipulation. *See Curling*, 334 F. Supp. 3d at 1314 (finding that plaintiffs had suffered an injury when a "DRE voting system was actually accessed or hacked multiple times already—albeit by cybersecurity experts who reported the system's vulnerabilities to state authorities, as opposed to someone with nefarious purposes."

(emphasis removed)). In such cases, the injury is to voters' "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." *Id.* at 1315. Put simply, states cannot refuse to "take[] steps to secure the DRE system from such attacks." *Id.* at 1316.

The evidence of cyberattacks on state election systems is not merely speculative; past cyberattacks and the substantial threat of future attacks have been demonstrated through recent legal proceedings against the cyber-attackers. In July 2018, Special Counsel Robert S. Mueller III issued an indictment against twelve Russian intelligence officers, accusing them of extensive cyberattacks targeting the November 2016 general election that included "attempts to break into state elections boards." Mark Mazzetti & Katie Benner, *12 Russian Agents Indicted in Mueller Investigation*, N.Y. Times (July 13, 2018), https://nyti.ms/2Clcn37. The indictment specifically alleged that Russian cyber-attackers "targeted state and county offices responsible for administering the 2016 U.S. elections." *United States v. Netyksho*, 1:18-cr-00215-ABJ (Indictment ¶ 75) (D.D.C. July 13, 2018).

Earlier this year, a joint intelligence bulletin issued by the Department of Homeland Security and Federal Bureau of Investigation confirmed that these Russian hacking activities targeted the election systems in all fifty U.S. states. *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. And in 2018 in Knox County, Tennessee, computers in foreign countries attacked the Knox County Election Commission server, 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.

While all DREs are vulnerable to these threats, Shelby County's voting system in particular has already proven susceptible to manipulation. 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. The subsequent conference report noted that many of these machines include

hardware components manufactured outside of the United States, which exposes voting machines to compromise "at the earliest stages in [the] manufacturing process." *Id.* at 15. "For example, foreign actors could design or plant a virus in software, memory, or even a small microchip that could affect an entire make/model of voting machine, theoretically allowing them to be compromised in one coordinated attack." *Id.*

That same study—which examined electronic voting nationwide—singled out other deficiencies in Shelby County's election system. In advance of the conference, hackers had purchased on eBay a Diebold ExpressPoll 5000, an electronic pollbook used in some localities to check in voters on Election Day. *Id.* at 12–13. That particular pollbook had been used in Shelby County, and because it was not properly decommissioned, hackers easily obtained the personal records—including names, addresses, dates of birth, and drivers' license numbers—of over 650,000 Shelby County voters. *Id.* Perhaps more concerning, the device had virtually no physical security protections, "allowing someone with a screwdriver to remove and replace the election media," which would effectively let a malicious actor disenfranchise every voter at a given polling location. *Id.*

These vulnerabilities have been publicly known for more than a decade. In the 2007 in-depth analysis of Diebold voting systems, including the AccuVote-TSx, commissioned by the California Secretary of State, experts from the University of

California, Berkeley, concluded that the system was not secure enough to guarantee the integrity of an election. Calandrino et al., *Source Code Review*. The experts found that "Diebold's general software engineering practices . . . are inadequate for meeting the rigorous security requirements of voting software." *Id*. at 29. They noted that the software "contains vulnerabilities that could allow an attacker to install malicious software on voting machines or on the election management system[, which] could cause votes to be recorded incorrectly or to be miscounted, possibly altering election results." *Id.* at i. Experts at Pennsylvania State University, the University of Pennsylvania, and WebWise Security, Inc., reached a similar conclusion when they analyzed the AccuVote-TSx DRE at the behest of Ohio's Secretary of State in 2007. They found that the election system "lacks the technical protections necessary to guarantee a trustworthy election under operational conditions" and that "[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 (2007), https://bit.ly/2K0FGfY (discussing flaws in the AccuVote-TSx and other elections systems made by Premier Election Solutions, the company formerly known as Diebold).

These vulnerabilities in the AccuVote-TSx DRE system are not merely hypothetical. 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., *Trust But Verify* at app. A, 75–76. This breach "allow[ed] unfettered remote access to the central tabulator to anyone connected to the county government network or the Internet." *Id.*

Shelby County remains at high risk for future election tampering because the County—as well as Tennessee more broadly—relies on voting equipment that cannot guarantee the accuracy or integrity of its elections. *See Stewart*, 444 F.3d at 855 (holding that the "increased probability that their votes will be improperly counted" because the state knowingly used outdated election technology made plaintiffs' injuries "neither speculative nor remote"). In a recent report on election security in all fifty states, the Center for American Progress gave Tennessee's voting system a grade of "F"—one of only five states to receive that failing grade—noting that "Tennessee's use of paperless DRE machines and insufficient post-election audit procedures leave the state open to undetected hacking and other Election Day problems." Danielle Root et al., *Election Security in All 50 States: Defending America's Elections* 165 (2018), https://ampr.gs/2pJwZ2m.

Shelby County's continued reliance on an antiquated machine—one that was was found unreliable twelve years ago and has only grown more obsolescent in the face of ever-evolving technological threats—more than warrants the F grade. The AccuVote-TSx DRE is "inadequate to ensure accuracy and integrity of the election

results." Calif. Sec'y of State, Withdrawal of Approval at 2; *see also* Green et al., *Trust But Verify* at 36. Shelby County's AccuVote-TSx DRE machines present a serious risk of ballot box tampering.

As one district court recently recognized, "[a]dvanced persistent threats in this data-driven world and ordinary hacking are unfortunately here to stay." *Curling*, 334 F. Supp. 3d at 1328. The best way to fight back against these threats is to accept "the research-based findings of national cybersecurity engineers and experts in the field of elections." *See id*. Those expert findings confirm that the vulnerabilities in Shelby County's AccuVote-TSx DRE election system are real, well known, and highly likely to cause further injury and risk of injury to Shelby County voters.

IV. Shelby County's Voting System Cannot Be Verifiably Audited to Address and Correct Errors and Vulnerabilities in Future Elections.

The deficiencies in Shelby County's system are compounded because Shelby County's system cannot be sufficiently audited. The *only* way to audit Shelby County's DREs is by using data. If the data itself is corrupted—whether by a software error, intentional interference, or some other source—then the audit will not shed light on the underlying problems.[5] *Cf.* Buell & Gay, *Is Technology the*

[5] Notably, although Shelby County does not use the printer attachment offered by the vendor to provide voters with a print-out of their choices, even the printer attachment is not reliable. *See* Green et al., *Trust But Verify* at 36 (noting that California declined to certify the AccuVote-TSx with printer attachment after finding a 10% error rate in a mock election of 96 machines).

Answer? at 39 (observing that an "inherent problem" with an analysis based only on data is that "there is no way to determine ground truth").

The inability to detect and correct software and data corruption in AccuVote-TSx DRE systems impairs the right to vote in two major ways. First, it virtually ensures that errors will reoccur from one election to the next by failing to detect those errors in the first place. *See Sandusky Cty. Democratic Party*, 387 F.3d at 574 (finding sufficient injury in fact where errors were "inevitable"). Second, and perhaps even more fundamentally, the inability to assess such flaws undermines public "[c]onfidence in the integrity of our electoral processes." *Hunter*, 635 F.3d at 234 (6th Cir. 2011) (quoting *Purcell v. Gonzalez*, 549 U.S. 1, 4 (2006)). Such confidence is "essential to the functioning of our participatory democracy." *Id.*; *see also Curling*, 334 F. Supp. 3d at 1328 ("A wound or reasonably threatened wound to the integrity of a state's election system carries grave consequences beyond the results in any specific election, as it pierces citizens' confidence in the electoral system and the value of voting.").[6]

[6] In an early case on which the Supreme Court relied for its holding in *Baker*, one of the offenses against the right to vote was "refusing to allow the supervisor of elections to inspect the ballot box, or even to enter the room where the polls were held." *Ex parte Siebold*, 100 U.S. 371, 379 (1879) (cited by *Baker*, 369 U.S. at 208). In other words, an injury to an election's integrity can frustrate the right to vote. The defendants' refusal to secure Shelby County elections against malicious attack and error undermines the election's integrity, particularly because an attack against the AccuVote-TSx likely would be undetectable.

"Election audits are critical to ensuring the integrity of election outcomes and for raising voter confidence." *See* Nat'l Acad. of Scis., Eng'g, and 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://bit.ly/36zvip5 (emphasis added). "As a result, errors and failures of the equipment may go undetected, which can lead to significant undetected errors in the vote tally." *Id*.

Shelby County's lack of a reliable auditing system compounds the errors that lead to unconstitutional voter dilution, ballot alteration, and ballot box tampering. But the addition of a reliable auditing system to an otherwise defective voting system

is not sufficient to *cure* other constitutional defects in the system. Shelby County must provide its voters with a system that is not rife with errors and vulnerable to manipulation; it must *also* ensure that the system may be audited using a reliable and voter-verified paper record. In other words, it must prevent stuffing and tampering with the ballot box, and then it must be capable of reliably demonstrating that its ballot boxes are in fact secure and identifying and correcting insecurities that may arise. Any less will risk the ongoing violation of the right to vote. These are not unattainable aspirations: they are requirements of a democratic voting process, *see Stewart*, 444 F.3d at 856–57 (explaining that the dilution of the right to vote through a variety of techniques have been determined to be unconstitutional and that alleged infringements of the right to vote must be "carefully and meticulously scrutinized" (quoting *Reynolds*, 377 U.S. at 562)), and furthermore, they are requirements that can be satisfied by election systems that are available and in use in Tennessee today.

CONCLUSION

For the foregoing reasons, the district court's order dismissing Plaintiffs' Complaint should be reversed, and the case should be remanded for further proceedings.

Respectfully submitted,

s/ *Megan C. Keenan*
Megan C. Keenan
John D. Graubert
Ryan Miller
Jeremy Patashnik
COVINGTON & BURLING LLP
850 Tenth St. NW
Washington, D.C. 20001
(202) 662-6000
MKeenan@cov.com
Counsel for NEDC and Individual Amici Curiae

s/ *Andrew Grosso*
Andrew Grosso
ANDREW GROSSO & ASSOCIATES
1101 Thirtieth Street NW, Suite 500
Washington, D.C. 20007
(202) 298-6500
Agrosso@acm.org
Counsel for the U.S. Technology Policy Committee of the Association for Computing Machinery

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

November 7, 2019

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitations of Federal Rules of Appellate Procedure 29(a)(5) and 32(a)(7)(B) because it contains 6,194 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in Times New Roman 14-point font.

s/ *Megan C. Keenan*
Megan C. Keenan
Counsel for Amici Curiae

November 7, 2019

CERTIFICATE OF SERVICE

I certify that on November 7, 2019, the foregoing document was filed electronically through the Court's CM/ECF system, which caused a true and correct copy to be served on:

Carol Chumney
Email: carol@carolchumney.law
5050 Poplar, Suite 2436
Memphis, TN 38157

Janet Kleinfelter
Email: Janet.kleinfelter@ag.tn.gov
P.O. Box 20207
Nashville, TN 37202

John L. Ryder
Email: jryder@harrisshelton.com
40 S Main Street, Suite 2210
Memphis, TN 38103

Pablo A. Verla
Email: pvarela@harrisshelton.com
40 S Main Street, Suite 2210
Memphis, TN 38103

s/ *Megan C. Keenan*
Megan C. Keenan
Counsel for Amici Curiae

November 7, 2019