IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE AT MEMPHIS

SHELBY ADVOCATES FOR VALID ELECTIONS; ET. AL,

Plaintiffs,

JURY TRIAL DEMAND

No. 2:18-cv-02706

TRE HARGETT in his Official capacity as TENNESSEE SECRETARY OF STATE; ET. AL,

Defendants.

PLAINTIFFS' MEMORANDUM OF LAW IN SUPPORT OF THEIR MOTION FOR PRELIMINARY INJUNCTION

COME NOW, the Plaintiffs Shelby Advocates for Valid Elections, Michael Kernell, Joe Towns, Sr., Ann Scott, Britney Thornton, [hereinafter the "Plaintiffs"], and file this Memorandum of Law in Support of their Motion for Preliminary Injunction against the Defendants and would state to the Court as follows:

I. FACTUAL BACKGROUND

On Friday, April 16, 2019, the Plaintiffs filed a Second Amended Complaint for Deprivation of Constitutional Rights, Injunctive Relief and Declaratory Relief, ECF 104, [hereinafter the "*SAC*"] against Defendants Tre Hargett, In his Official Capacity as Tennessee Secretary of State; Mark Goins, in His Official Capacity as the Coordinator of Elections for the State of Tennessee; The Tennessee Election Commission; Kent D. Younce, Judy Blackburn, Greg Duckett, Donna Barrett, James H. Wallace, Jr., Tom Wheeler, Mike McDonald, in each of their Official Capacity

as a Member of the Tennessee Election Commission; Linda Phillips, in Her Official Capacity as Administrator of the Shelby County Election Commission; Shelby County Election Commission; and Robert Meyers, Norma Lester, Dee Nollner, Steve Stamson, Anthony Tate, in each of their Official Capacity as a Board of Commission of the Shelby County Election Commission [hereinafter the "Defendants"]. The *SAC* is a civil rights action for declaratory and injunctive relief pursuant to 42 U.S.C. 1983, Rules 57 and 65 of the Federal Rules of Civil Procedure, and 28 U.S. C. 2201 and 2202. All of the Defendants have responded with Motions to Dismiss which are set for oral arguments on June 27, 2019. ECF 115, 116, 135.

Also pending is the Defendants' Motion to Stay Discovery, filed on April 8, 2019 only 2 days before the April 10, 2019 Status Conference, ECF 100; and the Plaintiffs' request for a forensic examination of a Shelby County Election Commission voting machines and tabulator. ECF 98. The Plaintiffs' filed a response in opposition to the Motion to Stay. ECF 106. The Court entered a text order holding the Motion and the ruling on a forensic examination in abeyance until June 20, 2019. ECF 101. The Status Conference was later rescheduled by the Court for June 27, 2019. ECF 135.

The Plaintiffs are seeking preliminary injunctive relief, among other things, for needed safeguards to be implemented by state and local election officials to protect the integrity of the vote in the upcoming October 3, 2019 municipal elections, as well as the federal, state, and local elections in 2020, and thereafter. One of the Plaintiffs, Britney Thornton, is seeking the office of City Council and will be on the ballot. She has a concrete and particularized injury if the hearing on the Plaintiffs' motion is not held expeditiously. ECF 104, No. 26. Early vote for the Memphis municipal elections will commence on September 13, 2019. And, the Tennessee U.S.

Presidential primaries are scheduled for March 3, 2020, with the general election in November 2020.

The Plaintiffs rely upon their verified *SAC* (with exhibits) in support of this Motion, and their briefs and exhibits filed in opposition to the Defendants' motions to dismiss the *SAC*, ECF 128, 130. The *SAC* describes the software, voting machines, equipment, systems and processes used presently in Shelby County, Tennessee. *SAC,* ECF 104, pgs. 25-37. The Defendants use GEMS software version 1.18.24.101 produced by Diebold to tabulate the votes, and AccuVote TSx version 4.6.4.103 [hereinafter "AccuVote DREs"] produced by Diebold, among other software and equipment. *SAC,* ECF 104, No. 75. The use of the AccuVote DREs makes Tennessee's elections unverifiable, unauditable, and vulnerable to undetectable manipulation. *SAC,* ECF 104, No. 108-129.

AccuVote DREs create no verifiable record of voter intent, paper ballot or paper verification of the votes cast, unlike optical scanner components that rely on a voter hand-marked paper ballot as a verifiable official record. *SAC,* ECF 104, No. 87, 98. The Shelby County AccuVote DREs were purchased in 2005, and were never recertified by the Defendants as required by Tenn. Code Ann. 2-9-117. *SAC*, ECF 104, No. 82. Even Defendant Administrator Phillips has testified before the Shelby County Commission that the vendor will no longer support the machines after 2020. Microsoft is no longer issuing updates or security patches for that software. *SAC*, ECF 104, No. 89.

Each Shelby County AccuVote DRE has a modem that allows it to be connected to a telephone jack for uploading results, and thus the capability to be connected to the internet and vulnerable to hacking. *SAC*, ECF 104, No. 86. The practice of the Defendants has been for the AccuVote DRE units to be used as an intermediate device for remote electronic transmission of

ballot data collected on the voting machines from designated Zone Turn-In sites to the Shelby County GEMS server, as observed by Plaintiff Kernell on November 8, 2018. *SAC,* ECF 104, No. 86.

The voting machines and electronic poll books are now in the Defendants' sole possession and control. These are the voting machines and system that do not have a paper ballot trail, have malfunctioned and flipped votes, and have been connected to the internet more than once despite warnings from a state agency and the vendor. ECF 104, No. 161-163. The Plaintiffs' *SAC* is rife with facts that warrant preliminary injunctive relief, such as the editing software found on the system with no explanation forthcoming from the Defendants, and the insecure transfer of votes with modems at satellite zones on election night. ECF 104, No. 161-163. The Defendants have failed to produce audit logs, refused to allow inspection of a voting machine, and have admitted that the system is outdated, insecure and vulnerable, yet failed to take prompt remedial action. ECF 104, No. 12. Statements are made to the public that are false by election officials on the evening news, such as that the system is not connected to the internet. Granting the relief requested by the Plaintiffs herein will provide needed transparency and cyber security protections.

In January 2017, the U.S. Department of Homeland Security (DHS) designated elections as "critical infrastructure" to more formally make election infrastructure "a priority for cybersecurity assistance and protections" and allow DHS to provide cybersecurity assistance to state and local election officials who request the same[1]. But, the Defendants have not replied as to whether they have even accessed these services.

[1] The DHS also launched its Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) in March 2018, which provides elections-focused cyber defense assistance to state and local elections offices nationwide. In 2018, the DHS announced that it provides at no cost to

In the fall of 2017, the State of Virginia decertified all DRE touchscreen voting machines requiring 23 cities and counties to purchase new voting machines only weeks before the November 2017 elections.[2]

In January 2018, the Congressional Task Force on Election Security issued a Final Report addressing the insecurity of the voting infrastructure in the United States. The Final Report stated:

> Given the breadth of security risks facing voting machines it is especially problematic that approximately 20% of voters are casting their ballots on machines that do not have any paper backup. These voters are using paperless Direct Recording Electronic (DRE) machines that have been shown over and again to be highly vulnerable to attack. Because these machines record votes on the internal memory of the machine, and do not leave any paper backup, it is near impossible to detect whether results have been tampered with.[3]

These findings are in accordance with those of research studies commissioned by the California Secretary of State and Ohio's Secretary of State regarding the Diebold AccuVote voting system. *SAC, Complaint, Nos. 101-108.*

As in the *Curling, etal v. Raffensperger, etal, No. 1:17-cv-2989 AT (N.D. Ga., Atlanta Division (hereinafter "Curling Order"),* these Plaintiffs' seek relief to require at a minimum hand-marked paper ballots with optical scans with no internet capability in all future elections

---

the state and local government and officials who request the following: cybersecurity assessments, such as cyber hygiene scanning, risk and vulnerability assessment, and cyber resilience reviews, cyber threat hunting and enhanced cyber services, 24/7 incident response, cybersecurity training among other services.

[2] https://politics.myajc.com/news/state--regional-govt--politics/judge-will-decide-whether-order-georgia-votersuse-paper-ballots/AZrL8megsykBm8zf5sbTJP/; The Washington Post, "Paper ballots make a come-back in Virginia this fall" October 7, 2017.

[3] Congressional Task Force of Election Security, *Final Report,* https://democratshomeland.house.gov/sites/democrats.homeland.house.gov/files/documents/ TFESReport.pdf.

held in Shelby County. *Curling, Order* of May 21, 2019, pg. 30, ECF 375. Recently revealed serious security vulnerabilities are set forth in the: (a) Congressional Task Force on Election Security's January 2018 Final Report; (b) Secretary of the U.S. Department of Homeland Security's March 2018 declaration that DRE voting systems are a 'national security concern'; (c) The May 2018 conclusion of the United States Senate Select Committee on Intelligence that DREs are 'at highest risk of security flaws" and that states "should rapidly replace outdated and vulnerable voting systems" with systems that have a verified paper trail; (c) the September 6, 2018 consensus report of the National Academies of Sciences, Engineering, and Medicine and associated National Research Council ("NAS"), titled "Securing the Vote: Protecting American Democracy," addressing the need to improve voting machine security, and recommending that voting machines that do not produce paper audit trails for each person's vote "should be removed from service as soon as possible" and that "[e]very effort should be made to use human-readable paper ballots in the 2018 federal election;" and (e) the 2018 resolution by the Board of Advisors of the U.S. Elections Assistance Commission (EAC) recommending that the EAC "not certify any system that does not use voter-verifiable paper as the official record of voter intent". *See Curling Order* of May 21, 2019, pg. 30. In August 2018, DHS Secretary Kirstjen Neilsen called on all state and local election officials to make certain that by the 2020 presidential election, every American votes on a verifiable and auditable ballot[4].

As set forth in *Curling Order* of May 21, 2019:

> The sea change between the issues raised in *Curling I* in 2017 and by September 2018 are highlighted most recently by the March 2019 Report on the Investigation Into Russian Interference in the 2016 Presidential Election by Special Counsel Robert S. Mueller. That Report, of which the Court takes judicial notice, documents successful efforts of Russian agents' cyber intrusions targeting

[4] *The Hill*, August 22. https://thehill.com/policy/cybersecurity/403148-dhs-chief-calls-onelection-officials-in-all-50-states-to-have.

the individuals and entities involved in the administration of U.S. elections. *See* Mueller Report: Section C(2.) Intrusions Targeting the Administration of U.S. Elections at 50-51. [5]

The State of Georgia uses the same Diebold AccuVote DREs as in Shelby County, Tennessee. ECF 104, No. 181. And, the U.S District Court, N.D. Ga. has held that the same AccuVote DRE voting systems used in Shelby County, were hacked multiple times by

[5] *Curling, Order of May 21, 2019, fn. 26, pg. 31* adds:
The Report found:
Victim included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities. The GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations. The GRU continued to target these victims through the elections in November 2016 [Redacted]…
By at least the summer of 2016, GRU officers sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities. GRU officers, for example, targeted state and local databases of registered voters using a technique known as "SQL injection," by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents). In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified.
GRU officers [Redacted]…scanned state and local websites for vulnerabilities. For example, over a two-day period in July 2016, GRU officers [searched] for vulnerabilities on websites of more than two dozen states [Redacted]..Similar [searches] for vulnerabilities continued through the election.
Unit 74455 also sent spearplishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of [Redacted] a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearplishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election. The spearplishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer. The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government.

cybersecurity experts who reported the system's vulnerabilities to the authorities. ECF 104, No. 181, fn. 64.

In addition, hacking activity meant to discredit Tennessee elections has already occurred in 2018 when Knox County experienced a distributed denial of service attack, distracting from the fact that hackers were infiltrating the election system and injecting malicious code into the system. ECF 104, No. 262 & Exb. X. On May 1, 2018, computers from about 65 countries accessed the Knox County website in a three-hour period, and an active attack was made on the server, with the election commission website crashing. ECF 104, No. 262.

The Plaintiffs contend that the custom and policy of the Defendants to use the GEMS outdated GEMS 1.18.24 software and AccuVote DREs in Shelby County violates their fundamental right to vote, and was purposefully designed and implemented with the intent of disenfranchising the large number of African American voters in Shelby County. *SAC,* ECF 104, Nos. 129, 180. It is important to note that the GEMS Reference manual produced by the Defendant Shelby County Election Commission states that the Vote Center Editor can be altered to cause programmed or uploaded memory cards [cartridges] to be lost, thus impacting on whether hundreds or thousands of votes are counted. *SAC,* ECF 104, No. 156.

The Plaintiffs document in their *Voting on Thin Ice* Report irregularities found with the Shelby County elections due to use of the GEMS 1.18.24 modified and outdated software and AccuVote DREs based upon five years of open records requests to the Defendants. *SAC,* ECF 104, Exb. "H". Among other things, the Report discusses documents produced by the Defendants that election databases are regularly sent via insecure methods to the vendor (even to Canada) which can compromise the data; results have been certified before the totals verified; a Certificate of Results submitted by the local election officials was accepted by the state election

officials with numbers not matching the tally tape; user names and passwords were emailed to state officials, and temporary staff have administrative rights to the election management system allowing them to make adjustments to the application; along with inadequate chain of custody of memory cards from the precincts to the Zone Turn-In sites which can allow for the insertion of malware to the system. *SAC,* ECF 104, Nos. 165-166, 171. .

Defendant Shelby County Election Commissioner Lester in an email to SAVE member Dr. Joseph Weinberg states that every night during early vote they could not get the totals to balance from the voting machines, and even mentions "rumors that ballots have been backed out". *SAC,* ECF 104, Nos 135, Exb. "L". Even the Defendant Secretary Hargett confirms in a letter to the State Comptroller that there have been a "series of errors in the Shelby County Election Commission stretching back at least a decade. Nearly every election cycle in the county in recent memory has been plagued by a myriad of errors and complaints of wrongdoing". *SAC,* ECf 104, No. 140, Exb. "A'". However, the Comptroller did not perform a forensic audit of the software and voting machines, instead only reviewing redistricting activities, *SAC,* ECF, 104, No. 145. .

The SAVE members have written the U.S. Department of Justice, and FBI more than once about their findings; testified before the Tennessee Election Commission in July 2018; and submitted their findings to the U.S Select Senate Intelligence Committee. *SAC,* ECF 104, No. 160, 183. However, the Shelby County voting systems are still in use, and apparently no forensic audit has been performed.

For several years, the Defendants did not conduct a complete audit of the precinct tally tapes with the tabulated results. Instead the auditor only compared a sample, contrary to Tenn. Code Ann. 2-8-104. *SAC,* ECF 104, No. 157. Also the Defendants will not produce the Shelby

County GEMS AVServer logs [audit trail] for review despite open records requests, contending that it is not a public record. *SAC,* ECF 104, No 158. .

A 2007 report of the Tennessee Advisory Commission on Intergovernmental Relations warned of unauthorized software found on the Shelby County voting systems that could allow manual editing of the GEMS database file, audit log, and election results. *SAC,* ECF 104, No. 162. *Complaint, No. 149.* More alarming was the finding that "someone was attempting to edit saved *ld* election summary reports, perhaps to agree with altered vote totals in the Diebold Microsoft Access database file". In addition, the report noted a critical security breach where unauthorized software had been installed which would allow "unfettered remote access to the central tabulator to anyone connected to the county government network or the Internet". The Report expressly states that "the GEMS central tabulator should absolutely NOT be connected to any network via Ethernet card, wireless network card, infrared port, USB port or modem". *SAC,* EC F 104, No. 162. In fact, Election Software & Systems ["ES &S] has now admitted that it installed remote-access software on systems sold in the states. [6]

An ES & S vendor report to the Defendant Shelby County Election Commission in 2013 stated that the tabulation server room was not secure, and had been plugged into the county network exposing it to hacking, virus and malware. *SAC,* ECF No. 104, No. 161. The 2013 ES & S report further found that the Shelby Board tabulation server room could be accessed by many people "which makes it difficult to defend against allegations of tampering". *SAC,*ECF 104, No. 161.

[66] "Top Voting Machine Vendor Admits it Installed Remote-Access Software on Systems Sold in States", Motherboard, 7/17/18. This is described in the article as the worst decision for security short of leaving ballot boxes on a Moscow street corner."
https://www.vice.com/en_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states

In the most recent November 2018 election, Myra Stiles, a former Shelby County Election Commissioner received the wrong ballot (which was observed as well by Memphis City Councilwoman Patrice Robinson). *SAC,* ECF 104, No. 177..Another citizen tried to vote for a candidate of one political party for Governor more than four times, but the AccuVote DRE showed that her vote was cast for a candidate of the other political party. *SAC,* ECF 104, No. 176.

The Defendant Shelby County Election Commission responded to the Plaintiffs' most recent open records requests that it has no documents regarding (1) persons having access to the tabulation server for the August 2, 2018 Shelby County Elections; (2) regarding the pre-election and post-election testing of the election computer at the Central Office [GEMS server] which received the tabulated votes from each election collection center zone [Zone Turn In Sites] for the August 2, 2018 Shelby County elections (including early vote), including checking for unauthorized software, unauthorized connection to the internet, hacking, and unauthorized editing of results; (3) regarding the chain of custody of the PCMCIA cards, ballots, poll books, election results cartridges for the Shelby County School Board District 9 election (including early vote); (4) regarding the access to the tabulator by the Election Systems & Software representative(s) from May 25, 2018 to August 6, 2018; (5) regarding any review of the software, tabulator, and/or voting machines used by Shelby County voters by independent expert(s), state, and/or federal official(s) and/or staff, since November 2016; (6) regarding any action taken in response to the *TACIR Trust But Verify* 2007 Staff Report, including documents that identify what person(s) put the editing software on the Shelby County Election Commission voting machines, as well as any investigation of the same, and the results of the investigation. *SAC,* ECF 104, No. 182, "M" & "N".

On September 30, 2018, the Plaintiffs SAVE faxed a demand letter to the Defendants Tennessee Secretary of State Tre Hargett, the State Board Members, the Coordinator of Elections, the Shelby Board Members, and the Shelby Administrator Linda Phillips asking, among other things, that the voting machines, software, and tabulators be inspected, and that they ask the U.S. Dept. of Homeland Security to provide a full cyber scan. *SAC*, ECF 104, No. 189. Only the Defendant Secretary and Goins have responded to the SAVE September 2018 demand, with a letter from the Coordinator of Elections. *SAC*, ECF 104, No. 190, "W".

In the October 4, 2018 letter, Goins attempts to wash his hands of the matter, stating that the Shelby County Election Commission is responsible for "protecting the technology used to conduct elections from malicious actors who want to jeopardize the integrity of the election process". *SAC*, ECF 104, "W". While he states that the Shelby County Election Commission has been educated and trained on cybersecurity and cyber-hygiene best practices, nowhere does he state whether or not any such best practices have been implemented, or that he is providing any oversite. *SAC*, ECF 104, "W".

In his October 4, 2018 letter, Goins denies the request for Plaintiff SAVE's expert to examine the Shelby voting systems, software, and tabulators. *SAC*, ECF 104, No. 191, "W". He contends that the chairs of the political parties, independent candidates and the press are notified when the voting machines are inspected and tested. *SAC*, ECF 104, N0. 191, "W". However, such inspection does not allow the party leaders, independent candidates or press to examine the internal software for the voting machines, and tabulator(s).

In his October 4, 2018 letter, Goins states that candidates can photograph poll tapes posted on the election precinct door after voting ends, but nowhere states that they will have the

opportunity to inspect the internal software for the voting machines and tabulator to ensure that the printed poll tapes accurately record a voter's ballot choices. *SAC,* ECF 104, No. 192, "W".

ARGUMENT AND AUTHORITIES

Under Fed. R. Civ. P. 65 (b), federal District Courts have broad discretion to grant preliminary injunctions. *See Connection Distribution Co. v. Reno,* 154 F.3d 281, 288 (6th Cir. 1998) and *Moltan Co. V. Eagle-Picher,* 55 F. 3d 1171, 1175 (6th Cir. 1995). The Court considers the following facts: "(1) whether the movant has a strong likelihood of success on the merits; (2) whether the movant would suffer irreparable injury without the injunction; (3) whether issuance of the injunction would cause substantial harm to others; and (4) whether the public interest would be served by issuance of the injunction". *Certified Restoration Dry Cleaning Network, LLC v. Tenke Corp.*, 511 F. 3d 535, 542 (6th Cir. 2007). The factors are to be balanced, and the district court is not required to make specific findings on each of the factors in deciding the motion for injunctive relief if fewer factors decide the issue. *See Jones v. City of Monroe, MI,* 341 F. 3d 474, 476 (6th Cir. 2003). At this stage, the plaintiffs need not prove their case in full. *Order Denying Motion for Temporary Restraining Order,* ECF, 43, pg. 5 [hereinafter "*Order"].*

The Supreme Court has held that "[i]t is beyond cavil that voting is of the most fundamental significance under our constitutional structure." *Burdick v. Takushi*, 504 U.S. 428, 433, 112 S. Ct. 2059, 119 L. Ed. 2d 245 (1992) (internal quotation marks omitted).

As the Supreme Court held in *Bush v. Gore*:

> The right to vote is protected in more than the initial allocation of the franchise. Equal protection applies as well to the manner of its exercise. Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another. . . . It must be remembered that "the right of suffrage can be denied by a debasement or dilution

> of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise."

531 U.S. 98, 104-05, 121 S. Ct. 525, 148 L. Ed. 2d 388 (2000) (internal citations omitted).

1. Plaintiffs Have a Strong Likelihood of Success on the Merits

As to the first factor under *Fed. R. Civ. P. 65,* the Plaintiffs have a strong likelihood of success on the merits. In their *SAC,* the Plaintiffs have more than raised questions going to the merits of their *Fourteenth Amendment* claims sufficient to make it a fair ground for litigation and thus for more deliberate investigation.

A. Due Process Claim

The impairment of voters' rights are actionable where the system is fundamentally unfair. *Order,* ECF 43, pg. 8. "Such a system could be found "where the entire election process including as part thereof the state's administrative and judicial corrective process fails on its fact to afford fundamental fairness." *Order* 43, pg. 8. Also, "where a state employs 'non-uniform rules, standards and procedures,' that result in significant disenfranchisement and vote dilution…" *Order* ECF 43, pg. 8 (*quoting League of Women Voters v. Brunner,* 548 F. 3d 463, 478 (6th Cir. 2008).

A United States District Court Judge in Georgia found a likelihood of success on the merits where the Plaintiffs sought a preliminary injunction to require paper ballots instead of DREs. *Curling, et. al v. Kemp, et. al, No. 1:17-cv-02989-AT,, Order, ECF. 309,* (N.D. Ga. Sept. 17, 2018). The Court held:

> Here, Plaintiffs have shown that their Fourteenth Amendment rights to Due Process and Equal Protection have been burdened. Put differently, the State's continued reliance on the use of DRE machines in public elections likely results in "a debasement or dilution of the weight of [Plaintiffs'] vote[s]," even if such conduct does not completely deny Plaintiffs the right to vote. *Bush v. Gore*, 531

U.S. 98, 105, 121 S. Ct. 525, 148 L. Ed. 2d 388 (2000) (quoting *Reynolds*, 377 U.S. at 555).

…Plaintiffs shine a spotlight on the serious security flaws and vulnerabilities in the State's DRE system — including unverifiable election results, outdated software susceptible to malware and viruses, and a central server that was already hacked multiple times.
…

As discussed earlier, the Curling Plaintiffs' voting-systems cybersecurity expert, Alex Halderman, demonstrated at the hearing how malware could be introduced into a DRE machine via a memory card and actually change an elector's vote without anyone knowing. (*See also* DeMillo Affidavit, Doc. 277 Ex. C; Buell Affidavit, Doc. 260-3; Bernhard Affidavit, Doc. 258-1 at 33-42.) Additionally, Professor Halderman explained in his testimony in detail the reasons why the DRE auditing and confirmation of results process used by state officials on a sample basis is generally of limited value. This process is keyed to matching the *total* ballots cast, without any independent source of individual ballot validation, and it can be defeated by malware similar to that used by the Volkswagen emissions software that concealed a car's actual emissions data during testing. (Halderman testimony at hearing; Halderman Affidavit, Doc. 260-2 ¶¶ 35-48; *see also* DeMillo Affidavit, Doc. 277, Ex. C ¶¶ 10-20.) Further, parallel testing of DREs is of limited value. "If the testing reveals, at the close of the election, that the machines were counting incorrectly, there will likely be no way to recover the true results, since the machines used in Georgia have no paper backup records." (Halderman Affidavit, Doc. 260-2 ¶ 41.)

Plaintiffs also emphasize current cybersecurity developments regarding election security and the heightened, legitimized concerns of election interference. Contrary to Defendants' assertions, Plaintiffs' claims do not boil down to paranoia or hypothetical fear. 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. Indeed, the evidence and testimony presented conforms with the patterns of heightened cybersecurity breach and data manipulation attacks now regularly appearing in civil financial cases as well as criminal cases.

…

Plaintiffs have so far shown that the DRE system, as implemented, poses a concrete risk of alteration of ballot counts that would impact their own votes. Their evidence relates directly to the manner in which Defendants' alleged mode of implementation of the DRE voting system deprives them or puts them at imminent risk of deprivation of their fundamental right to cast an effective vote (i.e., a vote that is accurately counted). *United States v. Classic*, 313 U.S. 299,

> 315, 61 S. Ct. 1031, 85 L. Ed. 1368 (1941); *Stewart*, 444 F.3d at 868. Plaintiffs' evidence also goes to the concern that when they vote by DRE, their vote is in jeopardy of being counted less accurately and thus given less weight than a paper ballot.

Curling v. Kemp, supra, Order, ECF. 309, pgs. 33-44. Shelby County, Tennessee uses the same AccuVote DRE voting machines and software as in Georgia. The *Curling* case is moving forward with discovery. *Curling Order, 5/21/19, ECF 375, pg. 61*. As in *Curling, supra*, the Plaintiffs have a strong likelihood of success on the merits on their constitutional deprivation claims.

And, the *SAC* sets out sufficient facts that are not "garden variety election irregularities" that could possibly occur with any type of voting system, and also significant evidence of disenfranchisement and fundamental unfairness as a result of the voting system in place. The Plaintiffs' expert Mathew Bernhard, states that due to architectural flaws of the system, and failures to provide operational security at many levels, it is not possible for any person to faithfully attest that any voting machine in the county is free from malware that can affect election results. ECF. 104, No. 223. He adds that use of this election system subjects votes to a substantial risk of election outcomes which do not fairly represent the political opinions of voters in Shelby County. ECF.104, No. 224. He also states that the transmission of election results over a network by the Defendants exposes the system to an even greater risk of compromise. ECF, 104,No. 225. Bernhard adds that the *SAC* does not allege "garden variety" or isolated errors. ECF. 104, No. 225, Exb "U".

Bernhard further avers that there is a substantial risk undetectable error and manipulation will continue to increase as voting equipment ages and foreign actors become more sophisticated and brazen in their attempts to impact elections in the U.S. ECF.104, No. 227 . He finds that

there is circumstantial evidence, based upon the Plaintiffs' complaint and the *Voting on Thin Ice Report,* that election tampering has occurred. ECF. 104, No. 231 & Exb. X.

In addition, the Plaintiffs' private data was exposed and sold on Ebay, as demonstrated at the DEF CON 2017 Hacking Conference. *SAC,* ECF 104, No. 233, Exb. "X", No. 28.

Thus, there is ample evidence that necessitates this Court's involvement.

And, while no balloting system is perfect, even the ES & S vendor has written to Congress that it will no longer sell the DRE non-paper trail voting machines, and urging Congress to pass a law requiring paper trails.[7] Thurs, the Plaintiffs' claims are not hypothetical, as corroborated by their expert Bernhard. And, unlike *Weber v. Shelley,* 347 F. 3d 1101 (9th Cir. 2003) decided some 16 years ago, there has been a sea of change since the 2016 Presidential election. And, more so, since the 2018 Knox County, Tennessee hacking incident.

Moreover, a ruling by this Court granting the Plaintiffs' Motion in whole, or in part, will not create a mad scramble to alter operations on the eve of early voting. There are three months until early vote commences for the October 2019 municipal elections, and 9 months before the March 2020 Tennessee Presidential primary. And, action by this Court will render the system and process more secure and reliable, providing greater voter confidence that malware is not lurking on the memory cards, tabulator, or voting machines; that votes will not be remotely transmitted thus opening up the system to manipulation; and an Independent Master to provide needed oversight. Without this Court stepping in, the Plaintiffs will be forced to vote on a

---

7 https://thehill.com/policy/technology/447784-top-voting-machine-manufacturer-urges-congress-to-make-paper-records

fundamentally unfair voting system. Thus, the Court should hear the proof, and order protections.

B. Equal Protection Claim

The Plaintiffs have alleged violation of the Equal Protection Clause of the Fourteenth Amendment because Shelby County, Tennessee voters are treated differently than those voters in the State using paper ballots. For example, Hamilton County uses hand-marked paper ballots with optical scanners. They also contend that because Shelby County has a disproportionately large number of African-American voters compared to other Tennessee counties, this voting system disproportionately impacts and disenfranchises those voters.

The Court should apply strict scrutiny under the *Anderson-Burdick* test. However, even under a rational basis standard, plenty of voters have been turned away from the polls and there is substantial evidence of votes not being properly counted. Thus, there is a severe restriction on the right to vote.

Weighing he Plaintiffs' injuries from using the current voting systems, equipment, and processes, against any interest asserted by the Defendants to continue with the present, it is clear that the Court should take action.

While Tennessee has allowed each county to determine which voting system to use on an approved list, it has failed to decertify the Shelby County system despite the warnings from the U.S Congress Intelligence Committee, federal government, and private renowned security experts. Moreover, the state has provided protections for counties using hand-marked paper ballots and optical scanners, but not required the same of the DRE machines and systems used in Shelby County. "A state having power to ensure uniform treatment of voters cannot adopt policies leading to disparate treatment of those voters and thereafter plead 'no control' as a

defense." *Bush*, 531 U.S. 98, 109 (2004). The willful blindness, malfeasance, and nonfeasance of the Defendants is evident.

This Court is needed in order to implement a constitutional balance of power between the Plaintiff voters and the state and local county election commission, and officials. The failures are so egregious that the voters can not assure that once they cast their vote and entrust its accurate delivery to the Defendants for tabulation, that nefarious and foreign unlawful intervention will not alter or cast it instead to cyberspace. And, the fact that the county in Tennessee with the largest population of African-American voters uses this voting system, along with the pattern in the county over many years of multiple irregularities, wrongdoings, and stonewalling as to the same, evidences the requisite discriminatory intent under the federal and Tennessee equal protection clauses as well as the need for this Court to protect the Plaintiffs' constitutional rights where all have failed to act.

2. **Other Factors.**

There is also a threat of irreparable injury warranting emergency injunctive relief. The Plaintiffs' injuries are set forth in their *SAC*, and also discussed at length in their brief in opposition of the State Defendants' Motion to Dismiss. ECF 128, pgs. 9-19. In *Curling, supra, Order, Dk. 309, pg. 40-*, the Court found:

> Turning to the second element for a preliminary injunction, the Court also finds that Plaintiffs have demonstrated a real risk of suffering irreparable injury without court intervention. … Absent an injunction, there is a threat that Plaintiffs' votes in the upcoming elections will not be accurately counted. Given the absence of an independent paper audit trail of the vote, the scope of this threat is difficult to quantify, though even a minor alteration of votes in close electoral races can make a material difference in the outcome.

As recently as November 2018, about 6000 voters were not found in the epoll books, thus creating barriers to those who were registered, sought to vote, but whose names were not located. ECF. 104, No. 8. The disenfranchisement was so great in Shelby County, in November 2018, that it was documented in the *Stateline* national article. ECF. 104, No. 11. The Tennessee Black Voter Project sued in October 2018, when half of the voter registration forms were rejected by the Defendant Shelby County Election Commission. ECF. 104, No. 206. And, in July 2018, a Chancellor issued an order for the Shelby County Election Commission to open more early voting sites and days earlier as a result of a lawsuit filed by the NAACP, after arguments that the plan to open only three sites in Germantown, East Memphis, and Whitehaven would have suppressed votes in predominately black neighborhoods. ECF. 104, No. 205.

In fact, the Court's action is urgently required to ensure a smooth election process in the October 2019 municipal elections, and the federal, state and local elections in Shelby County in 2020. As the Court acknowledges, "implementing more secure and adequate voting systems always advances the public interest". *Order,* ECF 43, pg. 15. And, in that there are several months before these elections, the relief requested will not interfere with the elections and instead will enhance the public's experience at the polls. Bernhard states that new paper based systems provide substantial mitigation to the risks facing voters in Shelby County. ECF. 104, No. 227, Exb."U", No. 7.

Undoubtedly, the public interest is served with stronger safeguards to protect the integrity of the vote. As explained in *Curling, supra, Order, Dk. 309, pg. 45,* with regard to those plaintiffs' motion for a preliminary injunction*:*

> Advanced persistent threats in this data-driven world and ordinary hacking are unfortunately here to stay. Defendants will fail to address that reality if they

> demean as paranoia the research-based findings of national cybersecurity engineers and experts in the field of elections. Nor will surface-level audit procedures address this reality when viruses and malware alter data results and evade or suppress detection[89].

3. Relief Requested

The Plaintiffs request that the Court immediately set a hearing on this Motion and permit the Plaintiffs to present expert and witness testimony, and introduce exhibits, and to order the relief requested as set forth in their Motion for Preliminary Injunction filed with this Memorandum in Support.

Respectfully submitted,

CAROL CHUMNEY LAW PLLC

/s/ Carol Chumney
Carol J. Chumney (#012021)
carol@carolchumneylaw.com
5050 Poplar, Suite 2436
Memphis, TN 38157
(901) 844-7141-office
(901) 537—7440- fax
Attorney for the Plaintiffs

8

https://thehill.com/policy/technology/447784-top-voting-machine-manufacturer-urges-congress-to-make-paper-records

9 Although the *Curling* Court denied the request of the plaintiffs that it order paper ballots to be used for the November 2018 elections, it found that "delay is not tolerable" in …confronting and tackling the challenges before the State's election balloting system. Further that "the Defendants and State election officials had buried their heads in the sand". *Id. at 45.*

CERTIFICATE OF SERVICE AND NOTICE PURSUANT TO FED. R. CIV. P. 65

The undersigned hereby certifies that a copy of the foregoing has been served upon:
Janet M. Kleinfelter
Matt Jones
Public Interest Division
Office of Attorney General
P.O. Box 20207
Nashville, TN 37202
Janet.kleinfelter@ag.tn.gov
Matt.jones@ag.tn.gov

John L. Ryder
Pablo A. Varela
HARRIS SHELTON HANOVER WALSH, PLLC
40 S. Main Street, Suite 2210
Memphis, TN 38103
jryder@harrisshelton.com
pvarela@harrisshelton.com

via U.S. Mail and ECF email on this 27 day of June 2019.

/s/Carol Chumney
Carol Chumney