



## **I. Introduction**

This case involves colliding election and voting rights dynamics and dilemmas. The State of Georgia Defendants have delayed in grappling with the heightened critical cybersecurity issues of our era posed for the State's dated, vulnerable voting system that provides no independent paper audit trail. The Plaintiffs did not bring their preliminary injunction motions in a sufficient time span to allow for thoughtful, though expedited, remedial relief, despite the important, substantive content of their evidentiary submissions in connection with their preliminary injunction motions. There are no easy answers to the conflicts posed here. In a democracy, citizens want to be assured of the integrity of the voting process, that their ballots are properly counted and not diluted by inaccurate or manipulated counting, and that the privacy of their votes and personal information required for voter registration is maintained. But citizens also depend on the orderly operation of the electoral and voting process. Last-minute, wholesale changes in the voting process operating in over 2,600 precincts, along with scheduled early voting arrangements, could predictably run the voting process and voter participation amuck. Transparency and accountability are, at the very least, essential to addressing the significant issues that underlie this case.

Currently before the Court in this matter are Defendants' motions to dismiss [Docs. 82, 83, 234] and Plaintiffs' more recently filed motions for preliminary injunction [Docs. 258, 260, 271]. Given the time sensitivity of Plaintiffs' motions with respect to the upcoming November 2018 elections, the Court held an extended

full-day hearing on Plaintiffs' motions on September 12, 2018 as well as the threshold jurisdictional issues of standing and Eleventh Amendment immunity raised in Defendants' motions to dismiss.<sup>1</sup> The Court, out of an abundance of caution, addressed the issues of standing and Eleventh Amendment immunity first and determined whether it could properly exercise jurisdiction over this case before considering Plaintiffs' request for emergency injunctive relief. After hearing argument on these issues, the Court announced orally its determination that it could properly exercise jurisdiction for purposes of proceeding with the hearing on Plaintiffs' preliminary injunction motions. The Court further announced that a written order would follow setting forth more specifically the basis for this finding. Accordingly, this Order addresses issues of standing and Eleventh Amendment immunity as well as Plaintiffs' motions for preliminary injunction.

---

<sup>1</sup> Defendants' motions to dismiss also raise other non-jurisdictional arguments that Plaintiffs have failed to state viable claims for relief and that their claims are barred by res judicata and collateral estoppel. The Court notes that only Fulton County Defendants move to dismiss based on collateral estoppel; the State Defendants do not move on this basis. With respect to res judicata and collateral estoppel in particular, Plaintiffs have effectively argued at this stage that their current claims are not barred. Moreover, even if a few Plaintiffs were deemed estopped, it appears that at least some Plaintiffs would still proceed with their claims. The Court will more fully address these and all other issues raised in Defendants' motions to dismiss in a separate, subsequent order.

## II. Background<sup>2</sup>

In their complaints, their motions for preliminary injunction, and their presentations during the September 12th hearing, Plaintiffs<sup>3</sup> paint an unsettling picture of the vulnerabilities of Georgia's voting system along with the recent, increased, and real threats of malicious intrusion and manipulation of the system and voter data by nation states and cyber savvy individuals.

Plaintiffs start by describing Georgia's voting system. The system relies on the use of Direct Recording Electronic voting machines ("DREs") for electors to cast their votes in public elections. This computer voting equipment is used in tandem with the State's Global Election Management Systems ("GEMS") server and County GEMS servers that communicate voting data.<sup>4</sup> DRE touchscreen computer voting machines are located at polling stations in every precinct during elections and are otherwise stored in various county facilities throughout the state. Electors use DRE machines if they are voting early and in-person with absentee ballots or if they are voting in-person on election day. "The voting machines are

---

<sup>2</sup> This section provides a brief factual summary based on the allegations in the Curling Plaintiffs' Second Amended Complaint (Doc. 70), the Coalition Plaintiffs' Third Amended Complaint (Doc. 226), the Curling Plaintiffs' Motion for Preliminary Injunction (Doc. 260), the Coalition Plaintiffs' Motion for Preliminary Injunction (Doc. 258), information presented during the September 12, 2018 hearing, and supplemental affidavits as well as Defendants' responses to Plaintiffs' filings.

<sup>3</sup> There are two sets of Plaintiffs in this case represented by separate counsel. Donna Curling, Donna Price, and Jeffrey Schoenberg are referred to as the "Curling Plaintiffs." The Coalition for Good Governance ("CGG"), Laura Digges, William Digges III, Ricardo Davis, and Megan Missett are referred to as the "Coalition Plaintiffs."

<sup>4</sup> A related software program is used to create the ExpressPoll pollbooks providing confidential voter identification information by precinct. Poll workers access this data by computer to verify voter registration and to create the DRE Voter Access Card that activates the specific electronic ballot on the DRE machine that should be linked to the voter's address.

computers with reprogrammable software.” (Halderman Affidavit, Doc. 260-2 ¶ 16.) The DRE machines record votes electronically on a removable memory card, and each card is later fed into the county GEMS server to tabulate the vote totals by candidate and the results of other ballot questions. When the polls have closed, poll workers prompt the DRE machines to internally tally the electronic total number of votes and print a paper tape of the vote totals per machine.

Most significantly, the DREs do not create a paper trail or any other means by which to independently verify or audit the recording of *each* elector’s vote. i.e., the actual ballot selections made by the elector for either the elector’s review or for audit purposes. Instead, at the hearing, Dr. Alex Halderman, a Professor of Computer Science and Engineering and Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, discussed and demonstrated how a malware virus can be introduced into the DRE machine by insertion of an infected memory card (or by other sources) and alter the votes cast without detection.<sup>5</sup> Dr. Halderman gave a live demonstration in Court with a Diebold DRE using the same type of equipment and software as that used in Georgia. The demonstration showed that although the same total number of votes were cast, the contaminated memory card’s malware changed the actual votes cast between candidates. There was no means of detection of this as the “malware modified all of the vote records, audit logs, and protective counters stored by the

---

<sup>5</sup> Dr. Halderman’s affidavit provides additional detail and context related to his testimony. (Doc. 260-2.)

machine, so that even careful forensic examination of the files would find nothing amiss.” (Halderman Affidavit, Doc. 260-2 ¶ 19.) The DRE machine’s paper tape simply confirmed the same total number of votes, including the results of the manipulated or altered votes. Viruses and malware have also been developed by cyber specialists that can spread the “vote stealing malware automatically and silently from machine to machine during normal pre- and post-election activities,” as the cards are used to interface with the County and State GEMS servers. (*Id.* ¶ 20.)

Other cybersecurity elections experts have shared in Professor Halderman’s observations of the data manipulation and detection concealment capacity of such malware or viruses, as well as the ability to access the voting system via a variety of entry points. Plaintiffs filed affidavits in the record for several of these experts.<sup>6</sup> Professor Wenke Lee (Professor of Computer Science at Georgia Tech and a member of a new study commission convened by the Secretary of State) also prepared a PowerPoint presentation summary on the topic for the Commission that identified this malware detection and manipulation capacity. (Pl. Ex 5, Preliminary Injunction Hearing.) Professor Halderman’s analysis of the severe limitations of the “logic and accuracy” and “parallel testing” auditing processes used by Georgia to test ballot counting are summarized in his affidavit and will be

---

<sup>6</sup> See DeMillo Affidavit, Doc. 277, Ex. C; Buell Affidavit, Doc. 260-3; Stark Affidavit, Doc. 296-1; Bernhard Affidavit, Doc. 258-1 at 33-42. Professor DeMillo, who also testified at the hearing, is the Chair of Computer Science at Georgia Tech and has served as Dean of the College of Computing at Georgia Tech and as Director of the Georgia Tech Center for Information Security.

discussed later. (Doc. 260-2 at ¶¶ 37-48.) Suffice it to say, at this juncture, that national- and state-commissioned research-based studies by cybersecurity computer scientists and elections experts consistently indicate that an independent record of an elector's physical ballot is essential as a reliable audit confirmation tool.

The DREs record individual ballot data in the order in which they are cast, and they assign a unique serial number and timestamp to each ballot. This design for recording ballots, according to Plaintiffs, makes it possible to match the ballots to the electors who cast them. Additionally, the Georgia DREs use versions of Windows and BallotStation (developed in 2005) software, both of which are out of date – to the point that the makers of the software no longer support these versions or provide security patches for them. (Halderman Affidavit, Doc. 260-2 ¶¶ 24-28.) The DRE machines and related election software are all the product of Premier Election Solutions, formerly known as Diebold Election Systems. A large volume of the voting machines were purchased when the DRE initiative was first implemented in the 2002 to 2004 period in Georgia.

Statewide, Georgia uses its central GEMS server at the Secretary of State's offices to build the ballots for each election for each county.<sup>7</sup> The central GEMS server communicates the election programming and other files onto the memory cards before an election. From 2002 to December 2017, the Secretary of State

---

<sup>7</sup> The ballot software also programs the location of candidates and other ballot options on the touchscreens of the DRE machines. Ballot adaptations, thus, are created for 159 counties and their over 2,600 precincts.

contracted with Kennesaw State University to maintain the central server for the State at a unit in the University called the Center for Election Services (“CES”). Plaintiffs allege that the central server was accessible via the internet for a time – at least between August 2016 and March 2017.

In August 2016, Logan Lamb, a professional cybersecurity expert in Georgia, went to CES’s public website and discovered that he was able to access key election system files, including multiple gigabytes of data and thousands of files with private elector information. The information included electors’ driver’s license numbers, birth dates, full home addresses, the last four digits of their Social Security numbers, and more. Mr. Lamb was also able to access, for at least 15 counties, the election management databases from the GEMS central tabulator used to create ballot definitions, program memory cards, and tally and store and report all votes. He also was able to access passwords for polling place supervisors to operate the DREs and make administrative corrections to the DREs. Immediately, Mr. Lamb alerted Merle King, the Executive Director overseeing CES, of the system’s vulnerabilities. The State did not take any remedial action after Mr. King was alerted.

In February 2017, a cybersecurity colleague of Mr. Lamb’s, Chris Grayson, was able to repeat what Mr. Lamb had done earlier and access key election information. Mr. Lamb also found, around this time, that he could still access and download the information as he had before. On March 1, 2017, Mr. Grayson notified a colleague at Kennesaw State University about the system’s

vulnerabilities, and this led to notification of Mr. King again. Days later, the FBI was alerted and took possession of the CES server.

The Secretary of State has since shut down the CES and moved the central server internally within the Secretary's office. But on July 7, 2017, four days after this lawsuit was originally filed in Fulton Superior Court, all data on the hard drives of the University's "elections.kennesaw.edu" server was destroyed. And on August 9, 2017, less than a day after this action was removed to this Court, all data on the hard drives of a secondary server – which contained similar information to the "elections.kennesaw.edu" server – was also destroyed. As discussed more fully later in this Order, the State offered little more than a one-sentence response to these data system incursions and vulnerabilities at CES.

The Premier/Diebold voting machine models at issue have been the subject of comprehensive critical review both by university computer engineer security experts independently as well as under the auspices of the States of Maryland, California, and Ohio. These studies identified serious security vulnerabilities in the software and resulted in the three states' adoption of different voting systems. (Halderman Affidavit, Doc. 260-2 ¶¶ 17-23; *see also* Atkeson Affidavit, Doc. 276-1 ¶¶ 8-9 (also discussing the states of New Mexico and Virginia transitioning away from DREs after identifying several issues with the machines).)<sup>8</sup>

---

<sup>8</sup> By contrast, the Secretary of State certified in April 2018 the accuracy and safety of the Georgia DRE system. This certification was based on a pre-announced examination of voting facilities and the conducting of a tiny mock election in several Georgia counties on November 27-29, 2017 by a combination of staff from the Secretary of State's Office and the Center for Election Services at Kennesaw State University. (Def. Ex. 2 from Preliminary Injunction Hearing.) No

Plaintiffs point to several national authorities which, in the last year, have raised the alarm about U.S. election security – and particularly about the use of DREs in elections. For instance, in March 2018, the Secretary of the U.S. Department of Homeland Security (DHS) declared DRE voting systems to be a “national security concern,” (Coalition Complaint, Doc. 258-1 at 10 n. 3) – approximately 14 months after the Department declared election systems to be “critical infrastructure” pursuant to 42 U.S.C. § 5195c.<sup>9</sup> (U.S. Department of Homeland Security, “DHS Cybersecurity Services Catalog for Election Infrastructure,” at 3.)<sup>10</sup> In May 2018, the Senate Select Committee on Intelligence concluded 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. (*Id.* at 11 n. 5.) And on September 6, 2018, after it was commissioned to consider the future of voting in the United States, the National Academies of Sciences, Engineering, and Medicine<sup>11</sup> and associated National

---

cybersecurity experts or computer engineering scientists are listed as participants in this review. There is no indication in the description of the examination that any effort was made to go beyond a simple running of the equipment and observation of election procedures to reach this determination. In other words, there is no indication that any effort was made to evaluate the trove of software and data security and accuracy issues identified in studies performed on behalf of other states or by cybersecurity and computer engineers in the field.

<sup>9</sup> Critical infrastructure is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Section 5195c(b) of the Critical Infrastructures Protection Act makes clear that information systems and their interdependence constitute a central concern of Congress.

<sup>10</sup> See [https://www.eac.gov/assets/1/6/DHS\\_Cybersecurity\\_Services\\_Catalog\\_for\\_Election\\_Infrastructure.pdf](https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf).

<sup>11</sup> Congress established the National Academies of Sciences, Engineering, and Medicine in 1863 as an independent body, which has the obligation to provide scientific and technical advice to any department of the Government upon request and without compensation. See

Research Council (“NAS”) issued a consensus report about the need to secure and improve state and local election systems.<sup>12</sup> The report, titled “Securing the Vote: Protecting American Democracy,” made a number of recommendations, including that “[e]very effort should be made to use human-readable paper ballots in the 2018 federal election.” (Doc. 285-1 at 35.) The report further recommended that voting machines that do not produce paper audit trails for each elector’s vote “should be removed from service as soon as possible” and that each state “should require a comprehensive system of post-election audits of processes and outcomes.” (*Id.* at 35-36.)

Similarly, the Board of Advisors of the U.S. Elections Assistance Commission (EAC) passed a resolution in 2018 recommending that the EAC “not certify any system that does not use voter-verifiable paper as the official record of voter intent.”<sup>13</sup>

Dr. Wenke Lee, Professor of Computer Science at Georgia Tech University and Co-Executive Director of the Institute for Information Security – the sole computer scientist appointed to the Secretary of State’s new Secure Accessible Fair Elections (“SAFE”) Commission – has echoed these same paper ballot and audit

---

<http://www.nasonline.org/about-nas/leadership/governing-documents/act-of-incorporation.html>.

<sup>12</sup> As noted by Professor Richard A. DeMillo in his supplemental affidavit, “a consensus report of the NAS . . . represents the highest authority that the U.S. Government can rely upon when it seeks to be advised on matters of science, technology and engineering.” (Doc. 285-1 ¶ 9.)

<sup>13</sup> See discussion of EAC action and audit outcome issues in the affidavit of Philip B. Stark, Professor of Statistics and Associate Dean of Mathematical and Physical Sciences and faculty member in Graduate Program in Computational Data Science and Engineering at University of California, Berkeley. (Doc. 296 ¶¶ 20-25.)

verification recommendations in his August 30, 2018 presentation on cybertechnology to the Commission. He has also stressed the essential need for installation on an ongoing basis of new hardware and software components designed to provide security protection to ensure voting system security. (Pl. Ex. 5, Preliminary Injunction Hearing.)

In the midst of the events involving the breach of the CES at Kennesaw State University, Plaintiffs filed the current case against Defendants<sup>14</sup> in August 2017. Plaintiffs essentially claim that the DRE voting system in Georgia is unsecure, is unverifiable, and compromises the privacy and accuracy of their votes, and therefore they claim that Defendants' continued use of the DRE system violates their constitutional rights. A brief overview of the particular claims brought by each set of Plaintiffs is instructive here.

The Coalition Plaintiffs bring two federal claims in their Third Amended Complaint:

(1) a 42 U.S.C. § 1983 claim for violation of the Fourteenth Amendment's guarantee of due process, based on the substantial burden placed on their fundamental right to vote; and

---

<sup>14</sup> Defendants are largely classified in two groups: (1) the "State Defendants," which include Brian Kemp in his official capacity, the State Election Board, and members of the State Election Board (David J. Worley, Rebecca N. Sullivan, Ralph F. Simpson, and Seth Harp) in their official capacities; and (2) the "Fulton County Defendants," which include Richard Barron in his official capacity, the Fulton County Board of Registration and Elections, and members of the Fulton County Board of Registration and Elections (Mary Carole Cooney, Vernetta Nuriddin, David J. Burge, and Aaron Johnson) in their official capacities.

(2) a 42 U.S.C. § 1983 claim for violation of the Fourteenth Amendment’s guarantee of equal protection, based on the more severe burdens placed on the Plaintiffs’ right to vote, right to freedom of speech and association, and the Georgia constitutional right to a secret ballot<sup>15</sup> as a result of Plaintiffs choosing to vote by DRE relative to other similarly situated electors choosing to vote another way.

For each of these claims, the Coalition Plaintiffs seek declaratory and injunctive relief against Brian P. Kemp in his official capacity as the Secretary of State of Georgia and as Chairperson of the State Election Board; the members of the State Election Board (David J. Worley, Rebecca N. Sullivan, Ralph F. “Rusty” Simpson, and Seth Harp) in their official capacities; and the members of the Fulton County Board of Registration and Elections (Mary Carole Cooney, Vernetta Nuriddin, David J. Burge, Stan Matarazzo, and Aaron Johnson) in their official capacities. The Coalition Plaintiffs’ Third Amended Complaint seeks a range of relief that is broader than their Motion for Preliminary Injunction now before the Court. Specifically, the Coalition Plaintiffs’ Third Amended Complaint seeks the following:

- A court order declaring it unconstitutional to conduct public elections using any DRE model,

---

<sup>15</sup> The Coalition Plaintiffs clarify, in their Response to the State Defendants’ Motion to Dismiss, that they are not bringing a state-law claim for violation of the Georgia Constitution. They are instead bringing a federal § 1983 claim based on unequal enforcement of state law.

- An injunction enjoining Defendants from enforcing O.C.G.A. § 21-2-383(b)<sup>16</sup> and Georgia State Election Board Rule 183-1-12-.01<sup>17</sup> and from requiring voters to cast votes using DREs,
- An injunction prohibiting Defendants from conducting public elections with optical scanned paper ballots without also requiring post-election audits of paper ballots to verify the results, and
- An injunction prohibiting Defendants from conducting public elections without also requiring subordinate election officials to allow meaningful public observation of all stages of election processing.

The Curling Plaintiffs bring essentially the same two constitutional claims as those brought by the Coalition Plaintiffs. As a slight variation, the Curling Plaintiffs bring their constitutional claims against the Defendants listed above as well as one additional defendant: Richard Barron in his official capacity as the Director of the Fulton County Board of Registration and Elections. The Curling

---

<sup>16</sup> “Notwithstanding any other provision of this Code section, in jurisdictions in which direct recording electronic (DRE) voting systems are used at the polling places on election day, such direct recording electronic (DRE) voting systems shall be used for casting absentee ballots in person at a registrar’s or absentee ballot clerk’s office or in accordance with Code Section 21-2-382, providing for additional sites.” O.C.G.A. § 21-2-383(b).

<sup>17</sup> “Beginning with the November 2002 General Election, all federal, state, and county general primaries and elections, special primaries and elections, and referendums in the State of Georgia shall be conducted at the polls through the use of direct recording electronic (DRE) voting units supplied by the Secretary of State or purchased by the counties with the authorization of the Secretary of State. In addition, absentee balloting shall be conducted through the use of optical scan ballots which shall be tabulated on optical scan vote tabulation systems furnished by the Secretary of State or purchased by the counties with the authorization of the Secretary of State; provided, however, that the use of direct recording electronic (DRE) voting units is authorized by the Secretary of State for persons desiring to vote by absentee ballot in person.” Ga. Comp. R. & Regs. r. 183-1-12-.01.

Plaintiffs also seek somewhat varied relief for these claims in their Second Amended Complaint:

- A court order declaring that Defendants violated the Fourteenth Amendment, and
- An injunction prohibiting Defendants from using DREs or other voting equipment that fails to satisfy state requirements.<sup>18</sup>

As stated above, both sets of Plaintiffs seek more limited and immediate relief in their motions for preliminary injunction. The Curling Plaintiffs ask the Court to order the following relief prior to the November 2018 general election: (1) enjoin the State Defendants to direct all counties that the use of DREs in the November 2018 election (and the December 2018 runoff election) is prohibited, with the exception for electors with disabilities; (2) enjoin the State Defendants to direct all counties to conduct elections using paper ballots; and (3) require the State Defendants to promulgate rules requiring and specifying appropriate procedures for conducting manual audits of election results. Similarly, the Coalition Plaintiffs ask the Court to: (1) prohibit Defendants from conducting the November 2018 election (and the December 2018 runoff election) with DRE

---

<sup>18</sup> Additionally, the Curling Plaintiffs bring a state-law claim under O.C.G.A. § 9-6-20 for a writ of mandamus ordering Defendants to discontinue the use of DRE machines and to either use (a) an optical scanning voting system or (b) hand-counted paper ballots. The Curling Plaintiffs seek a writ of mandamus against the following Defendants: the members of the State Election Board in their official capacities; the State Election Board; Richard Barron in his official capacity as the Director of the Fulton County Board of Registration and Elections; the members of the Fulton County Board of Registration and Elections in their official capacities; and the Fulton County Board of Registration and Elections.

machines for in-person voting; (2) order Defendants to conduct such elections using paper ballots, as permitted by Georgia law, with certain exceptions made for persons with disabilities; (3) order the State Election Board Members to promulgate rules requiring and specifying appropriate procedures for conducting manual audits of election results; and (4) order the Secretary of State, before October 1, 2018, to audit and correct any identified errors in the DRE system's electronic pollbook data that will be used in both such elections.

The Court now turns to the jurisdictional issues raised in Defendants' motion to dismiss before addressing the Plaintiffs' motions for preliminary injunction.

### **III. Threshold Jurisdictional Issues**

#### **A. Standing**

The State Defendants argue that both the Curling Plaintiffs and the Coalition Plaintiffs lack standing to bring their claims in federal court. According to the State Defendants, Plaintiffs fail to establish each of the three elements required for standing. The Fulton County Defendants' Motion to Dismiss incorporates by reference the State Defendants' arguments on standing. (*See* Fulton Mot. to Dismiss, Doc. 82-1 at 5.)

The Supreme Court has set forth the standard for determining whether a party has standing:

It is by now well settled that the irreducible constitutional minimum of standing contains three elements. First, the plaintiff must have suffered an injury in fact—an invasion of a legally protected interest

that is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of. . . . Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

*United States v. Hays*, 515 U.S. 737, 742–43 (1995) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–561 (1992)) (internal quotation marks omitted). “[A] plaintiff must demonstrate standing for each claim he seeks to press and for each form of relief that is sought.” *Town of Chester, N.Y. v. Laroe Estates, Inc.*, 137 S. Ct. 1645, 1650 (2017) (quoting *Davis v. Federal Election Comm’n*, 554 U.S. 724, 734 (2008)).

As to the first element, Defendants contend that Plaintiffs have not sufficiently alleged a concrete “injury in fact.” Defendants argue that Plaintiffs’ allegations that the DRE voting machines are vulnerable to hacking and are “presumed to be compromised” convey only a speculative, generalized fear, thus falling short of establishing a concrete injury.

These arguments are unavailing. For one, Plaintiffs have alleged that the 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. (Curling Complaint, Doc. 70 ¶¶ 42-43, 45-49; Coalition Complaint, Doc. 226 ¶¶ 95-106.) Contrary to Defendants’ characterizations, Plaintiffs’ allegations are not premised on a

theoretical notion or “unfounded fear”<sup>19</sup> of the hypothetical “possibility” that Georgia’s voting system might be hacked or improperly accessed and used. Plaintiffs allege that harm has in fact occurred, specifically to their fundamental right to participate in an election process that accurately and reliably records their votes and protects the privacy of their votes and personal information. (Curling Complaint, Doc. 70 ¶ 14 (“Curling also chose to exercise her right to cast her vote using a verifiable paper ballot in the Runoff, so as to ensure that her vote would be permanently recorded on an independent record. To do so, Curling persisted through considerable inconvenience – only to be incorrectly told by Defendants Kemp and the Fulton County Board of Registration and Elections that she had not, in fact, cast a ballot, creating irreparable harm that her ballot was not counted.”); ¶ 16 (Donna Price “cast her vote on a DRE in the 2016 General Election,” and “[w]ithout the intervention of this Court, Price will be compelled to choose between relinquishing her right to vote and acquiescing to cast her vote under a system that violates her right to vote in absolute secrecy and have her vote accurately counted”); ¶ 38 (“DREs produce neither a paper trail nor any other means by which the records of votes cast can be audited.”); ¶¶ 42-43 (“Lamb was able to access key components of Georgia’s electronic election infrastructure . . . . In accessing these election system files, Lamb found a startling amount of private information,” including driver’s license numbers, birth dates, and the last four digits of Social

---

<sup>19</sup> See State Defendants’ Motion to Dismiss Coalition Plaintiffs’ Third Amended Complaint, Doc. 234-1 at 1.

Security numbers); Coalition Complaint, Doc. 226 ¶ 152 (member of CGG, Brian Blosser, “was prohibited from voting on April 18, 2017 . . . when his name did not appear on the eligible voter rolls” for the Sixth Congressional District and “was instead erroneously listed” as a resident of another district, an error that Fulton County Board members blamed on a “software glitch”); ¶ 154 (members of CGG, Mr. and Ms. Digges, previously in 2017 “chose to vote by mail-in paper absentee ballot because they were aware that an electronic ballot cast using an AccuVote DRE was insecure,” and they “were required to undergo the inconvenience of requesting paper ballot[s] and the cost of postage to mail their ballots” “well before Election Day”); ¶ 72 (“Georgia’s AccuVote DREs do not record a paper or other independent verifiable record of the voter’s selections.”); ¶ 92 (“[D]esign flaws render the electronic ballots cast on AccuVote DREs capable of being matched to voter records maintained by pollworkers and pollwatchers,” and thereby expose citizens’ candidate selections to poll workers); ¶ 97 (“Lamb freely accessed files hosted on the ‘elections.kennesaw.edu’ server, including the voter histories and personal information of all Georgia voters . . . . Lamb noted that the files had been publicly exposed for so long that Google had cached (i.e., saved digital backup copies of) and published the pages containing many of them.”); ¶ 138 (“Fulton Board Members have adopted voting procedures under which individual electronic ballots bearing a unique identifier are transmitted from Fulton County’s AccuVote DREs located in satellite voting centers to Fulton County’s central GEMS tabulation server in clear text (i.e., unencrypted) over an ordinary, unsecured

telephone line on Election Night. This practice violates fundamental security principles because it subjects the transmitted votes to manipulation (such as man-in-the-middle interception and substitution of votes) and exposes the votes with their unique identifier to third-party interception, violating voters' rights of secrecy in voting.”.)

Plaintiffs also allege the threat of future harm. For instance, in upcoming elections, Plaintiffs allege that Defendants are requiring them to vote early, mail a paper absentee ballot, and pay for postage to avoid having to use unsecure DRE machines, thereby subjecting them to unequal treatment. Furthermore, Plaintiffs plausibly allege a threat of a future hacking event that would jeopardize their votes and the voting system at large. Despite being aware of election system and data cybersecurity threats and vulnerabilities identified by national authorities and the DRE system's vulnerability to hacking as early as August 2016 – when Logan Lamb, the computer scientist, first alerted the State's Executive Director of the CES of his ability to access the system – Defendants allegedly have not taken steps to secure the DRE system from such attacks. (Curling Complaint, Doc. 70 ¶ 46 (“[N]ot only did Georgia fail to take remedial action when alerted to the problem Lamb raised, it failed to act even in the face of the detailed information on the cybersecurity threats facing the nation's election systems, and the recommended specific steps to reduce the risk, which were disseminated by the FBI, the DHS and

the EAC<sup>20</sup>.”); Coalition Complaint, Doc. 226 ¶ 112 (“[N]o efforts have been made to remediate the compromised software programs and machines or to identify and remove any malware that was likely introduced during the lengthy security breaches referred to herein on the ‘elections.kennesaw.edu’ server that hosted the election-specific software applications and data that are re-installed on every piece of voting and tabulation equipment used to conduct Georgia’s elections in advance of each election conducted using Georgia’s Voting System.”).)

Importantly, courts have recognized these sorts of alleged harms as concrete injuries, sufficient to confer standing. In particular, courts have found that plaintiffs have standing to bring Due Process and Equal Protection claims where they alleged that their votes would likely be improperly counted based on the use of certain voting technology. *See, e.g., Stewart v. Blackwell*, 444 F.3d 843, 855 (6th Cir. 2006) (“The increased probability that their votes will be improperly counted based on punch-card and central-count optical scan technology is neither speculative nor remote.”), *vacated* (July 21, 2006), *superseded*, 473 F.3d 692 (6th Cir. 2007) (vacated and superseded on the grounds that the case was rendered moot by the county’s subsequent abandonment of the DRE machines at issue); *Banfield v. Cortes*, 922 A.2d 36, 44 (Pa. Commw. Ct. 2007) (finding that the plaintiffs had sufficiently alleged standing under similar Pennsylvania law, based on “the fact that Electors have no way of knowing whether the votes they cast on a

---

<sup>20</sup> DHS is the acronym for the U.S. Department of Homeland Security, and EAC is the acronym for the U.S. Election Assistance Commission.

DRE have been recorded and will be counted,” which “gives Electors a direct and immediate interest in the outcome of this litigation”); *c.f. Stein v. Cortes*, 223 F. Supp. 3d 423, 432-33 (E.D. Pa. 2016) (where plaintiffs sought a vote recount, post-election, based on the use of unsecure DREs, finding no standing based on the plaintiffs’ “less than clear” allegations that the DRE machines are “hackable”; that the Pennsylvania Election Code’s recount provisions are “labyrinthine, incomprehensible, and impossibly burdensome”; and that the past vote count was inaccurate – which plaintiffs merely posed as a “seemingly rhetorical question”).

Turning to causal connection, the second element of standing, Defendants raise different arguments in response to the Curling Plaintiffs’ claims versus the Coalition Plaintiffs’ claims. For the Curling Plaintiffs, Defendants argue that any injury would be traced to illegal hacking into the DREs, not the use of the DREs themselves. Here, as discussed above, the Curling Plaintiffs have alleged that Defendants were aware of serious security breaches in the DRE voting system and failed to take adequate steps to address those breaches. Notably, even after Mr. Lamb first alerted the State about his access of the voting system, he and another cybersecurity expert were able to access the system *again* about six months later. (Curling Complaint, Doc. 70 ¶ 47.) Plaintiffs allege that Defendants have continued to fail to take action to remedy the DRE system’s vulnerabilities. (*Id.* ¶¶ 46, 61, 62, 72.) And they allege that this failure, in turn, impacts the integrity of the voting system and their ability as citizens to rely upon it when casting votes in this system. (*Id.*) At the motion to dismiss stage, these allegations plausibly show

causal connection, even if indirectly, between Defendants' continued use of unsecure DREs and the injury to Plaintiffs' constitutional rights. *Focus on the Family v. Pinellas Suncoast Transit Auth.*, 344 F.3d 1263, 1273 (11th Cir. 2003) (“[E]ven harms that flow indirectly from the action in question can be said to be ‘fairly traceable’ to that action . . .”).

For the Coalition Plaintiffs, Defendants make the same argument above regarding causation (which fails) and another slightly different argument. Defendants take issue with the Coalition Plaintiffs' request for relief enjoining the State Defendants from enforcing O.C.G.A. § 21-2-383(b) and State Election Board Rule 183-1-12-.01. Defendants assert that the State Defendants (the Secretary and the State Election Board) do not mandate the use of DREs; rather, state law requires the use of DREs. Defendants maintain that the State Defendants are merely implementing the governing state law, which they are bound to do, and therefore Plaintiffs miss the mark by seeking to enjoin the State Defendants' actions instead of challenging the state law itself. In this way, Defendants argue that Plaintiffs have not linked their injury to any action by the State Defendants.

But O.C.G.A. § 21-2-383(b) does not *require* the use of DREs as Defendants claim it does. The statute requires absentee electors who vote in-person in the advance voting period to vote by DRE, but only “in jurisdictions in which direct recording electronic (DRE) voting systems are used at the polling places on election day.” The statute simply specifies the use of DREs under certain circumstances. Rather, it is the State Election Board that issued a rule requiring

the use of DREs in “all federal, state, and county general primaries and elections, special primaries and elections, and referendums,” and requiring the use of DREs by “persons desiring to vote by absentee ballot in person.” Ga. Comp. R. & Regs. r. 183-1-12-.01. When read together, the state statute and the State Election Board rule indicate that the State Defendants have chosen to enforce state law so as to generally require the use of DREs in elections statewide.

Even apart from the statutory language, the Coalition Plaintiffs have plausibly alleged that the State Defendants play a critical role in directing, implementing, programming, and supporting the DRE system throughout the state. The Coalition Plaintiffs allege that the Secretary provided the counties with the DRE machines and the software on which they operate. (Coalition Complaint, Doc. 226 ¶ 59.) Additionally, from 2002 to December 2017, the Secretary allegedly contracted with Kennesaw State University to create the Center for Election Services (“CES”) “to assist the Secretary in the fulfillment of his statutory duties to manage Georgia’s election system.” (*Id.* ¶ 93.) The CES maintained a central computer server containing sensitive voting-related information such as software applications, voter registration information, ballot building files, and “other sensitive information critical to the safe and secure operation of Georgia’s Voting System.” (*Id.* ¶¶ 94, 119.) These factual allegations, when considered with the Third Amended Complaint as a whole, show that the Coalition Plaintiffs have alleged enough of a causal link between the State Defendants’ conduct and their injury for standing purposes.

Finally, on the third element of redressability, Defendants raise some of the same arguments as they do for the second element. Defendants argue that an injunction prohibiting the State Defendants from using DREs would not actually stop the deployment of DREs. Defendants maintain that county officials not included in this suit would continue to use DREs, as the State is not the entity that enforces the law requiring DREs. Defendants also argue that a different balloting system would not eliminate potential third-party interference, as no election system is flawless.

As stated above, the Court finds that the Coalition Plaintiffs have sufficiently alleged that the State Defendants play a significant role in the continued use and security of DREs, and therefore the requested injunction would help redress some of the Coalition Plaintiffs' injury. The Secretary of State both has the authority and obligation to investigate complaints regarding the accuracy and safety of the DRE voting system and to take appropriate corrective action in connection with the continued use of the DRE system. O.C.G.A. § 21-2-379.2. The Third Amended Complaint describes how the Secretary of State could play a critical role in conducting an in-depth investigation and formulating a remedy. As alleged in the Complaint, the State of California commissioned a study in 2007 to examine the security of its own Diebold AccuVote DRE system, the same type of system used in Georgia. Upon the study's findings that the DRE system was inadequate, had serious design flaws, and was susceptible to hacking, California's Secretary of State then decertified its DRE system in 2009. (Coalition Complaint, Doc. 226 ¶¶ 81,

84, 86.) The Complaint similarly alleges that the Secretary of State for Ohio commissioned an independent expert study of a newer version of the DREs than those used in Georgia and reached similar conclusions as to the lack of trustworthy design and vulnerability to attack of the election system. (*Id.* ¶¶ 81, 83, 85.)

The State Defendants here are similarly in a position to redress the Plaintiffs' alleged injury. Thus, if the Court were to grant at least part of the requested injunctive relief as to the suspended use of the DRE voting system, any injunction would likely enjoin both the State Defendants as well as the Fulton County Defendants (as there is no argument that the County would not be enjoined). Furthermore, as to Defendants' argument that no election system is flawless, the Coalition Plaintiffs rightly point out that this is not the standard for redressability. Plaintiffs are seeking relief to address a particular voting system which, as currently implemented, is allegedly recognized on a national level to be unsecure and susceptible to manipulation by advanced persistent threats through nation state or non-state actors. Plaintiffs are not asking for a system impervious to all flaws or glitches.

Defendants assert three additional arguments related to standing: that the Coalition Plaintiffs cannot manufacture standing by inflicting harm on themselves, that the individual Plaintiff Coalition for Good Governance ("CGG") lacks organizational and associational standing, and that Plaintiffs must reside in the jurisdiction for which they seek to enjoin DRE use.

The first of these arguments fails because the cases relied on by Defendants are distinguishable. Here, the Coalition Plaintiffs are suffering injury from the voluntary exercise of their *fundamental right to vote*, not from just any sort of activity that they decide to engage in. In *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), the plaintiffs voluntarily spent money to take certain protective measures, based on a hypothetical fear of being subject to surveillance. And in *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992), the plaintiffs expressed an intent to voluntarily return to certain places they had visited before, which would deprive them of the opportunity to observe animals of an endangered species. These activities do not invoke the protection associated with exercising fundamental rights, such as the right to vote. The Coalition Plaintiffs aptly point out that Defendants' logic would bar many voting rights cases, based on individuals choosing to vote by one method or another, which certainly is not how courts have assessed standing in this context.

Defendants' challenge of CGG's standing similarly fails. "An organization has standing to enforce the rights of its members when its members would otherwise have standing to sue in their own right, the interests at stake are germane to the organization's purpose, and neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Fla. State Conference of N.A.A.C.P. v. Browning*, 522 F.3d 1153, 1160 (11th Cir. 2008) (internal quotation marks omitted). The State Defendants argue that the Coalition Plaintiffs merely "presume" harm to their own members, without sufficiently

alleging harm to one or more of their members. (State Mot. to Dismiss, Doc. 234-1 at 31.) They also argue that CGG cannot assert that individuals are “members” merely because they are listed on CGG’s mailing list. (*Id.*) The Coalition Plaintiffs, however, have alleged that the individual Plaintiffs – Laura Digges, William Digges III, Ricardo Davis, and Megan Missett – are all members of CGG. Contrary to Defendants’ assertion, these particular Plaintiffs do not allege that they are members of CGG solely because they are on the mailing list. Furthermore, at least one of these Plaintiffs also alleges harm to his or her individual rights under the federal Constitution, as discussed above, so that they could presumably sue Defendants in their own right. (Coalition Complaint, Doc. 226 ¶¶ 24-27.) The Court finds these allegations sufficient to confer associational standing to CGG.<sup>21</sup>

As for Defendants’ argument that Plaintiffs must reside in the county where they seek injunctive relief, this argument misses the mark. The Court need only find that one plaintiff (from each of the two sets of Plaintiffs) has sufficiently alleged standing, and that is the case here. *Am. Civil Liberties Union of Fla., Inc. v. Miami-Dade Cty. Sch. Bd.*, 557 F.3d 1177, 1195 (11th Cir. 2009) (“Because Balzli has standing to raise those claims, we need not decide whether either of the organizational plaintiffs also has standing to do so.”). Specifically, the Curling Plaintiffs allege that Donna Curling is a resident of Fulton County and intends to vote in the upcoming elections in Fulton County. (Curling Complaint, Doc. 70 ¶

---

<sup>21</sup> The Court need not reach Defendants’ challenge to CGG’s *organizational* standing, as the Court has already found the Coalition Plaintiffs sufficiently alleged *associational* standing for CGG. *See Common Cause/Georgia v. Billups*, 554 F.3d 1340, 1351 (11th Cir. 2009).

13.) The Coalition Plaintiffs likewise allege that Megan Missett is a resident of Fulton County who intends to vote in the County's upcoming elections. (Coalition Complaint, Doc. 226 ¶ 27.) Based on the current allegations, both Ms. Curling and Ms. Missett have established the required elements of injury in fact, causation, and redressability as discussed above.

In sum, the Court finds that both sets of Plaintiffs have sufficiently alleged standing to bring their claims at this juncture.

### **B. Eleventh Amendment Immunity**

Defendants argue that Plaintiffs' two federal claims are barred by the Eleventh Amendment. Defendants acknowledge the *Ex Parte Young*<sup>22</sup> exception to Eleventh Amendment immunity, which allows claims against state officers in their official capacities for prospective injunctive relief. But Defendants assert that the exception does not apply here for the following reasons: Plaintiffs seek to enjoin the enforcement of a state law that they do not challenge as unconstitutional; Plaintiffs have not alleged an ongoing or continuous violation of federal law; Plaintiffs seek to remedy past, not prospective, conduct; and Plaintiffs' requested relief implicates special state sovereignty interests.

Defendants' arguments are meritless. First, Plaintiffs rightly point out that the *Ex Parte Young* exception applies to as-applied challenges to state statutes, not just facial challenges as Defendants imply. Here, Plaintiffs specifically challenge the application of Georgia's law by Defendants to require in-person voting by DRE.

---

<sup>22</sup> 209 U.S. 123 (1908).

Second, Plaintiffs clearly allege an ongoing and continuous violation of federal law. The injunctive relief they request is designed to prevent injury by enjoining the use of DREs in upcoming elections and other future elections. Third, and likewise, Plaintiffs seek to remedy prospective harm.<sup>23</sup> Fourth, the requested relief does not implicate special state sovereignty interests by essentially usurping the State's role in regulating elections. Plaintiffs are not asking the Court to direct how the State counts ballots. They are asking the Court to bar the use of DREs based on the specific circumstances, history, and data security issues presented in this case and where the State has alternative options of using optical scanners and hand counting ballots. And they seek to require the State to implement a fully auditable ballot system designed to ensure the accuracy and reliability of the voting process in this challenging era when data system vulnerabilities pose a serious risk of opening election data, processes, and results to cyber manipulation and attack.

Thus, pursuant to *Ex Parte Young*, the Court finds that the Eleventh Amendment does not bar Plaintiffs' federal claims.<sup>24</sup>

For the reasons stated above, the Court finds that it has jurisdiction at this juncture for purposes of considering Plaintiffs' motions for preliminary injunction.

---

<sup>23</sup> Defendants' arguments opposing Plaintiffs' motions for preliminary injunction belie this argument, as Defendants claim that the requested injunctive relief, if granted, would harm them on the eve of the *upcoming* November 2018 election.

<sup>24</sup> At one point, State Defendants cite to cases involving state sovereign immunity issues. The Court clarifies that state sovereign immunity is not at issue here – only Eleventh Amendment sovereign immunity. Plaintiffs do not allege violations of the Georgia Constitution. They allege violations of the U.S. Constitution based in part on the enforcement of state law requiring the use of DREs for in-person voting. (*See* SEB Rule 183-1-12-.01.)

The Court therefore **DENIES IN PART** Defendants' Motions to Dismiss [Docs. 82, 83, 234] as discussed herein.

#### **IV. Plaintiffs' Motions for Preliminary Injunction**

To obtain preliminary injunctive relief, the moving party must show that: (1) it has a substantial likelihood of success on the merits; (2) irreparable injury will be suffered unless the injunction issues; (3) the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and (4) if issued, the injunction would not be adverse to the public interest. *McDonald's Corp. v. Robertson*, 147 F.3d 1301, 1306 (11th Cir. 1998). In the Eleventh Circuit, "[a] preliminary injunction is an extraordinary and drastic remedy not to be granted unless the movant clearly established the 'burden of persuasion' as to the four prerequisites." *Id.* (internal citations omitted).

Furthermore, the Supreme Court has recognized that there are special considerations involved with impending elections and the critical issues at stake.

In *Reynolds v. Sims*, the Court stated:

[O]nce a State's [election-related] scheme has been found to be unconstitutional, it would be the unusual case in which a court would be justified in not taking appropriate action to insure that no further elections are conducted under the invalid plan. However, under certain circumstances, such as where an impending election is imminent and a State's election machinery is already in progress, equitable considerations might justify a court in withholding the granting of immediately effective relief in a legislative apportionment case, even though the existing apportionment scheme was found invalid. In awarding or withholding immediate relief, a court is entitled to and should consider the proximity of a forthcoming election and the mechanics and complexities of state election laws, and should act and rely upon general equitable principles.

377 U.S. 533, 585 (1964); *see also Purcell v. Gonzalez*, 549 U.S. 1, 4–5 (2006) (holding that courts are “required to weigh, in addition to the harms attendant upon issuance or nonissuance of an injunction, considerations specific to election cases and its own institutional procedures”).

Considering the totality of the evidence and affidavits presented at this juncture, the Court finds with a measure of true caution that Plaintiffs are likely to satisfy the first element for a preliminary injunction – a likelihood of success on the merits – for at least some of their claims. The Court’s caution is that though the parties have filed endless briefs on Defendants’ multiple motions to dismiss and amended complaints, largely due to Plaintiffs’ changes in counsel, the case did not move substantively forward until the motions for preliminary injunction were filed in August 2018. The subject matter in this suit is complex, even if well-presented, and there is still key information that needs to be gathered. For instance, the voting system and data handling deficiencies in one county, Fulton County, could possibly impact all other counties in the state. The State also never called the Chief Information Officer for the Secretary of State’s Office to testify, and substantive answers from other state officials were limited by their lack of computer science expertise and apparent knowledge. In short, the case would benefit from some discovery and a full evidentiary hearing on the merits over several days.

That said, 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 (1992) (internal quotation marks omitted). The Court goes on to recognize that “[i]t does not follow [] that the right to vote in any manner and the right to associate for political purposes through the ballot are absolute.” *Id.* Thus, courts apply a more flexible standard in this context:

A court considering a challenge to a state election law must weigh the character and magnitude of the asserted injury to the rights protected by the First and Fourteenth Amendments that the plaintiff seeks to vindicate against the precise interests put forward by the State as justifications for the burden imposed by its rule, taking into consideration the extent to which those interests make it necessary to burden the plaintiff’s rights. . . . Under this standard, the rigorousness of our inquiry into the propriety of a state election law depends upon the extent to which a challenged regulation burdens First and Fourteenth Amendment rights. Thus, as we have recognized when those rights are subjected to severe restrictions, the regulation must be narrowly drawn to advance a state interest of compelling importance. . . . But when a state election law provision imposes only reasonable, nondiscriminatory restrictions upon the First and Fourteenth Amendment rights of voters, the State’s important regulatory interests are generally sufficient to justify the restrictions.

*Id.* at 434 (internal quotation marks omitted).

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 (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. Mirroring the truncated affidavit statement of Merritt Beaver, the Chief Information Officer in the Office of the Secretary of State, the State Defendants' response brief merely states, without more, that the central server is no longer an issue because the way Kennesaw State University maintained the system "is not the way that those tasks are undertaken now." (*See* Response, Doc. 265 at 22; Beaver Affidavit, Doc. 265-1.) The Defendants presented no witness with actual computer science engineering and forensic expertise at the preliminary injunction hearing to address the impact of the Kennesaw State University breach or the specifics of any forensic evaluation of the servers, DREs, removable media used for transfer of data, analog phone modems, and other connected devices that together constitute the election system. The Defendants' response brief is close to non-responsive to the concerns that Plaintiffs raise about the serious vulnerability of the server and the election data system at large to intrusion, virus, or attack. Defendants' response is bare-boned in the absence of evidence of installation of updates to software or equipment or evidence of statewide software and hardware scrubbing – after at least one or more portions of the database system operated by Kennesaw State University was left accessible for at least six months. In fact, Defendants presented scant evidence to rebut Plaintiffs' expert evidence regarding Georgia's persistent failure to update or

replace software systems, despite security flaws identified by the software industry.<sup>25</sup>

Michael Barnes, the Director of the CES at Kennesaw State University,<sup>26</sup> was the sole staff member at the CES to move over to the State when the Center's functions were taken over by the Secretary of State's office. He in turn became the Center's Director once this transfer occurred. The State presented his testimony at trial. Mr. Barnes professed effectively no knowledge about the ramifications for the state's voter system or remedial measures in connection with Mr. Lamb's accessing the CES's voter registration databases – which was filled with millions of voter records with personally identifiable information, passwords for election day supervisors, and the software used to create ballot definitions, memory cards, and vote tabulations. Mr. Barnes also appeared not to recognize the full scope of the contamination risks posed by his own use of a plug-in USB drive (which he connects both to the central GEMS “air-gapped” server and his own “public facing” computer that is connected to the Internet) to transfer vital elections programming data to the counties. Mr. Barnes similarly did not appear to recognize the risks associated with the use of analog phone connections for the transfers of election results.

---

<sup>25</sup> Indeed, after Fulton County experienced a meltdown in the tabulation of the vote in the primary for the Sixth Congressional District in 2017, Richard Barron, the Director of Registration and Elections for Fulton County, vocally expressed his view that the software system of 2000 vintage should be investigated and should have been replaced. (Pl. Ex. 9, Preliminary Injunction Hearing.)

<sup>26</sup> Mr. Barnese is not a computer scientist.

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.<sup>27</sup> 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.<sup>28</sup>

Defendants assert that the state election laws at issue are “narrowly drawn to effect the State’s regulatory interest in maintaining fair, honest and efficient elections.” (Response, Doc. 265 at 15.) This conclusory re-statement of an overarching principle of Fourteenth Amendment voting jurisprudence<sup>29</sup> does not by itself answer the issues before the Court. However, the Court recognizes the important policy changes and objectives achieved by the State’s adoption via the Secretary of State’s Office of the statewide integrated DRE voting system in approximately 2002. But the DRE system also originally was intended to include the capacity for an independent paper audit trail of every ballot cast, and this feature was never effectuated. (Report of the 21st Century Voting Commission, Pl. Ex. 10 at 38, introduced at Preliminary Injunction hearing; testimony of Cathy Cox.)

---

<sup>27</sup> The PowerPoint presentation of Dr. Wenke Lee, the sole cybersecurity scientist serving on the Secretary of State’s new SAFE Commission, identifies similar overarching risks and solutions, including paper ballots as durable evidence of election results. (Pl. Ex. 5 at Preliminary Injunction Hearing.)

<sup>28</sup> But in contrast to the circumstances where there is no independent vote audit trail, when money is stolen through cybercrime, ultimately the theft is clearly obvious – the funds are gone.

<sup>29</sup> See *Burdick*, 504 U.S. at 433.

As the Court noted at the preliminary injunction hearing, rapidly evolving cybertechnology changes and challenges have altered the reality now facing electoral voting systems and Georgia's system in particular. And it is this reality that Plaintiffs substantiated with expert affidavits and testimony as well as an array of voter affidavits and documentation. Defendants sidestep the fact that Georgia is only one of five states that rely on a DRE voting process that generates no independent paper ballot or audit record. Yet the Plaintiffs' evidence as to the problems of security, accuracy, reliability, and currency of Georgia's system and software have hardly been rebutted by Defendants except via characterizations of the issues raised as entirely hypothetical and baseless. Ultimately, an electoral system must be accurate and trustworthy. The State's apparent asserted interest in maintaining the DRE system without significant change cannot by itself justify the burden and risks imposed given the circumstances presented. *Burdick*, 504 U.S. at 434.

Plaintiffs are substantially likely to succeed on the merits of one or more of their constitutional claims, though this finding is a cautious, preliminary one, especially in light of the initial state of the record. 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 (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.<sup>30</sup> 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 (2000) (internal citations omitted).

The Defendants rely on *Wexler v. Anderson*, 452 F.3d 1226 (11th Cir. 2006) in maintaining that Plaintiffs cannot establish the viability of their Fourteenth Amendment claims described above. But *Wexler* and this case are distinguishable. The Eleventh Circuit noted that the *Wexler* plaintiffs "did not plead that voters in touchscreen counties are less likely to cast effective votes due to the alleged lack of a meaningful manual recount procedure in those counties," and therefore their "burden is the mere possibility that should they cast residual ballots, those ballots will receive a different, and allegedly inferior, type of review in the event of a manual recount." *Id.* at 1226. *Wexler* distinguishes this situation from the one in

---

<sup>30</sup> Plaintiffs allege other theories under these constitutional claims, including that their right to cast a secret ballot is violated and that they must incur greater costs to cast an absentee ballot if they choose to avoid voting by DRE. Plaintiffs may be less likely to prevail on these theories, though the Court will not reach that conclusion now, especially given the incomplete status of the evidentiary record.

*Stewart v. Blackwell*, 444 F.3d at 868-72, where strict scrutiny was applied based on the plaintiffs’ allegations of “vote dilution due to disparate use of certain voting technologies.” 444 F.3d at 871. Thus, in contrast with *Stewart*, the Eleventh Circuit in *Wexler* did not apply strict scrutiny and instead reviewed “Florida’s manual recount procedures to determine if they are justified by the State’s ‘important regulatory interests.’” *Wexler*, 452 F.3d at 1233 (citing *Burdick*, 504 U.S. at 434)).

Here, Plaintiffs appear to present facts that fall somewhere between *Wexler* and *Stewart*. Unlike *Wexler*, Plaintiffs are alleging that they are less likely to be able to cast accurate or effective ballots when voting by DRE. The evidence here is not as well developed as that in *Stewart*, which was decided on a fully factually developed summary judgment record. Still, Plaintiffs in this case have presented sufficient evidence so far that their votes cast by DRE may be altered, diluted, or effectively not counted on the same terms as someone using another voting method – or that there is a serious risk of this under the circumstances.

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. This analysis to some extent parallels the “injury in fact” standing analysis above. 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.

Finally, the Court considers together the last two factors in evaluating whether preliminary injunctive relief should be granted: whether the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and, if issued, whether the injunction would not be adverse to the public interest. The Court considers these factors in tandem, as the real question posed in this context is how injunctive relief at this eleventh-hour would impact the public interest in an orderly and fair election, with the fullest voter participation possible and an accurate count of the ballots cast.

*This assessment involves a true catch-22.*

While Plaintiffs have shown the threat of real harms to their constitutional interests, the eleventh-hour timing of their motions and an instant grant of the paper ballot relief requested could just as readily jeopardize the upcoming elections, voter turnout, and the orderly administration of the election. Defendants introduced substantial evidence from Elections Directors from counties with major populations (e.g., Fulton, Cobb, Gwinnett, Muscogee, and Richmond Counties) regarding the fiscal, organizational, and practical impediments and burdens associated with a court order that would require immediate implementation of paper ballot and ballot scanning voting systems for the 2018 election cycle. (*See* Testimony of Richard Barron at Preliminary Injunction Hearing; Doc. 265-3; Doc. 265-6.) Various representatives of the

Secretary of State's office provided testimony regarding similar organizational and fiscal challenges. Some of these concerns, such as authority for emergency purchase orders of ballot paper or scanners, clearly are resolvable based on emergency purchase provisions under state and local law. The Court's greater concern, in considering the evidence, is that the massive scrambling required to implement such injunctive relief in roughly 2,600 precincts and 159 counties will seriously test the organizational capacity of the personnel handling the election, to the detriment of Georgia voters.

Plaintiffs have submitted evidence from various jurisdictions in other states of their ability to smoothly roll out a paper ballot/optical scanning system in an expedited time frame as well an affidavit from the administrator overseeing Maryland's transition over an expedited, but still far longer, time frame. The challenges presented in these jurisdictions are not comparable to managing a rapid implementation of a balloting system, associated technology, and administrative transition in less than seven weeks on a statewide basis in large population centers as well as tiny ones simultaneously. Nor is it likely simple to roll out a paper ballot system with proper, efficient scanning, when many polling station personnel throughout the state have never handled this scope of a paper ballot exercise – or used accompanying scanners on a massive basis.

Further, early elections begin mid-October. This poses an even earlier deadline for action and organization. Fulton County's Elections Director testified that the County would only be able to cope with the challenges of an immediate

ballot requirement by limiting early voting to one central location, rather than offering it at 20 locations spread throughout the county. This, of course, would likely directly impact voter turnout and access to voting.

Ultimately, any chaos or problems that arise in connection with a sudden rollout of a paper ballot system with accompanying scanning equipment may swamp the polls with work and voters – and result in voter frustration and disaffection from the voting process. There is nothing like bureaucratic confusion and long lines to sour a citizen. And that description does not even touch on whether voters themselves, many of whom may never have cast a paper ballot before, will have been provided reasonable materials to prepare them for properly executing the paper ballots.

The Court attempted to expedite this case at earlier times to no avail. The Court understands some of the reasons why Plaintiffs may have been unable to file a preliminary injunction motion before new counsel for the Coalition Plaintiffs filed a Third Amended Complaint in June 2018. But the *August* filing of their motion for preliminary injunction effectively put the squeeze on their proposed remedial relief. Requiring injunctive relief on this broad of a scale, and on an abrupt, time-limited basis, would likely undermine a paper ballot initiative with a scanned audit trail that appears in reality to be critically needed.

Meanwhile, the State Defendants have also stood by for far too long, given the mounting tide of evidence of the inadequacy and security risks of Georgia's DRE voting system and software. The Court is gravely concerned about the State's

pace in responding to the serious vulnerabilities of its voting system – which were raised as early as 2016 – while aging software arrangements, hardware, and other deficiencies were evident still earlier. The Secretary of State’s Secure, Accessible, & Fair Elections (SAFE) Commission has held just two meetings since its establishment in April 2018, though it is tasked with making recommendations to the legislature that convenes in January 2019. The State and the County’s arguments about the time and resource constraints at issue, in the event the Court granted the requested injunctive relief, are compelling right now, with the November election just weeks away. But these arguments only weaken the more that time passes and if Defendants continue to move in slow motion or take ineffective or no action. For upcoming elections after November 2018, Defendants are forewarned that these same arguments would hold much less sway in the future – as any timing issues then would appear to be exclusively of Defendants’ own making at that point.

Upon considering the totality of the evidence in connection with the four factors that must guide the Court’s determination regarding the grant of extraordinary relief as to Plaintiffs’ constitutional claims, the Court finds that the Plaintiffs have not carried their burden of persuasion to establish these prerequisites for such extraordinary injunctive relief in the immediate 2018 election time frame ahead.

## V. Conclusion

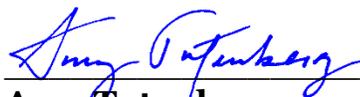
While Plaintiffs' motions for preliminary injunction [Docs. 258, 260, 271] are **DENIED**, the Court advises the Defendants that further delay is not tolerable in their confronting and tackling the challenges before the State's election balloting system. The State's posture in this litigation – and some of the testimony and evidence presented – indicated that the Defendants and State election officials had buried their heads in the sand. This is particularly so in their dealing with the ramifications of the major data breach and vulnerability at the Center for Election Services, which contracted with the Secretary of State's Office, as well as the erasure of the Center's server database and a host of serious security vulnerabilities permitted by their outdated software and system operations.

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.

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. The parties have strongly intimated that this case is headed for immediate appeal. But if the case stays with or comes back to this Court, the Court will insist on further proceedings moving on an expedited

schedule. The 2020 elections are around the corner. If a new balloting system is to be launched in Georgia in an effective manner, it should address democracy's critical need for transparent, fair, accurate, and verifiable election processes that guarantee each citizen's fundamental right to cast an accountable vote.

**IT IS SO ORDERED** this 17th day of September, 2018.



---

**Amy Totenberg**  
**United States District Judge**