ELECTRONICALLY FILED
5/19/2022 8:18 PM
03-CV-2022-900595.00
CIRCUIT COURT OF
MONTGOMERY COUNTY, ALABAMA
GINA J. ISHMAN, CLERK

IN THE CIRCUIT COURT OF

MONTGOMERY COUNTY, ALABAMA

Lynda Blanchard, Tommy Hanes,

Plaintiffs,

v.

John H. Merrill, as Alabama Secretary of State, Bill English, Wes Allen, Clay Crenshaw, Jeff Elrod, Will Barfoot, as members of the Alabama Electronic Voting Committee,

Defendants.

COMPLAINT

I. INTRODUCTION

1. This is a civil rights action for declaratory and injunctive relief, or in the alternative, for a writ of mandamus, to prohibit the use of electronic voting machines in the State of Alabama, as discussed herein, in the upcoming Election slated to be held on November 8, 2022 (the "2022 Election").

2. Through this Action, Plaintiffs seek an Order that Defendants collect and count votes through a constitutionally acceptable process, which relies on tried and true precepts that mandates integrity and transparency. This includes votes cast by hand on verifiable paper ballots that maintains voter anonymity; votes counted by human beings, not by machines; and votes counted with transparency, and in a fashion observable to the public.

3. The use of unsecure and fatally compromised black box electronic voting machines violates the rights of Plaintiffs and their fellow voters and office seekers. These machines undermine public confidence in the validity of election results. Just as the government cannot insist on "trust me," so too, private companies that perform governmental functions, such as vote reading and counting, cannot be trusted without transparent systems open to public scrutiny and validation.

4. Plaintiffs have a statutory right to have their ballots, and all ballots cast together with theirs, read and counted accurately and transparently, so that only legal votes determine the winners of each office contested in the 2022 Election. Electronic voting machines cannot be deemed reliably secure and do not meet the constitutional and statutory mandates to guarantee a free and fair election.

5. This Complaint is not an attempt to undo the past. Most specifically, it is not about undoing the 2020 presidential election. It is only about the future – about upcoming elections that will employ unsecure voting machines designed and run by private companies, performing a crucial governmental function, that refuse to disclose their software and system components and subject them to public evaluation. It raises the profound constitutional issue: can government avoid its obligation of democratic transparency and accountability by delegating a critical governmental function to private companies? Plaintiffs submit that the answer to this question is "no."

II. PARTIES

6. Plaintiff Lynda Blanchard ("Blanchard") is a candidate for Governor of Alabama. In that capacity, Blanchard has standing to bring this action as an aggrieved

person. Blanchard further has standing as an intended voter in the 2022 Election and as a qualified elector in Alabama.

7. Plaintiff Tommy Hanes ("Hanes") is a member of the Alabama House of Representatives, currently representing District 23. Hanes seeks re-election to that office in the 2022 Election, and therefore has standing to bring this action as an aggrieved person. Hanes further has standing as an intended voter in the 2022 Election and as a qualified elector in Alabama.

8. Defendant Merrill ("Merrill") is the Alabama Secretary of State. In that capacity, Merrill is the chief election officer in Alabama. Ala. Code § 17-1-3(a). Merrill is, through this Complaint, sued for prospective declaratory and injunctive relief in his official capacity as the Secretary of State of Alabama, together with any successor in office automatically substituted for Defendant Merrill by operation of Alabama Rule of Civil Procedure 25(d).

9. Defendants English, Allen, Crenshaw, Elrod, and Barfoot are the sitting members of the Alabama Electronic Voting Committee (collectively "Committee Defendants"). See Ala. Code § 17-7-22. In that capacity, the Committee Defendants are charged by statute with, among other duties:

- Publicly examining all makes of electronic vote counting systems submitted and certifying whether such systems comply with Alabama law;

- Ensuring that vote counting systems used Alabama are only certified after a satisfactory evaluation and testing has been performed to determine that the equipment meets the requirements of this article and performance and test standards for electronic voting systems issued by the Federal Election Commission"; and

- Re-examining previously certified electronic voting systems where a change or "improvement" to those systems is sought by a county.

Ala. Code § 17-7-23.

10. The Committee Defendants are also charged by statute with the duty "to recommend procedures to be implemented by the Secretary of State under the Administrative Procedure Act where appropriate to achieve and maintain the maximum degree of correctness and impartiality of voting, counting, tabulating, and recording votes, by electronic vote counting systems." Ala. Code § 17-7-25(a).

III. JURISDICTION AND VENUE

11. The Court has personal jurisdiction over all Defendants, each of whom is a resident and citizen of the State of Alabama.

12. This Court has subject matter jurisdiction because this action seeks to protect rights under the laws of the State of Alabama.

13. This Court has authority to grant declaratory relief based on §§ 6-6-220 through 6-6-232 of the Code of Alabama and Rule 57 of the Alabama Rules of Civil Procedure.

14. This Court has jurisdiction and authority to grant injunctive relief under Rule 65 of the Alabama Rules of Civil Procedure.

15. This Court further has jurisdiction and authority to grant injunctive relief because this action seeks such relief on constitutional grounds. *See, e.g.*, *Working v. Jefferson Cnty. Election Comm'n*, 2 So. 3d 827, 837 (Ala. 2008). ("'this court is committed

to the proposition that equity will interfere by injunction to restrain elections not authorized by law.'") (quoting *Dennis v. Prather*, 212 Ala. 449, 452, 103 So. 59, 62 (1925)).

16. Venue is proper in this Court because the events and omissions giving rise to Plaintiffs' claims occurred in Montgomery County. *See* Ala. Code § 6-3-2. Venue is also proper in this Court because this action involves the breach of official duties of officers of the State of Alabama who reside in Montgomery County.

IV. FACTUAL ALLEGATIONS

17. At present, every county in Alabama intends to tabulate votes cast in the 2022 Elections through optical scanners, the vast majority of which are manufactured by Election Systems & Software ("ES&S").

18. After votes are tabulated at the county level using these machines through these companies' proprietary election management systems, the vote tallies will be uploaded over the internet to an election reporting system.

19. Some voters in Alabama will rely on electronic voting systems to cast their votes as well as tabulate them. Voters who may have hearing or visual impairments may cast their votes with the aid of electronic ballot marking devices manufactured primarily by ES&S. These voters' electoral choices are even more vulnerable to attack and manipulation, as ballot marking devices pose significant security risks on their own.

20. All optical scanners and ballot marking devices certified by Alabama, as well as the software on which they rely, have been wrongly certified for use in Alabama and should not be used in the 2022 Election. These systems are potentially unsecure, lack adequate audit capacity, fail to meet minimum statutory requirements, and deprive voters

of the right to have their votes counted and reported in an accurate, auditable, legal, and transparent process. Using them in the upcoming elections, without objective validation, violates the voting rights of every Alabaman.

21. All electronic voting machines and election management systems, including those slated to be used in Alabama in the 2022 Election, have shown to be susceptible to manipulation through internal or external intrusion to alter votes and vote tallies.

22. Substantially similar vulnerabilities in electronic voting machines in general have been identified and publicized in analyses presented to various congressional committees. All electronic voting machines can be connected to the internet or cellular networks, directly or indirectly, at various steps in the voting, counting, tabulating, and/or reporting process.

23. Voting machines and systems used in Alabama contain electronic components manufactured or assembled in foreign nations which have attempted to manipulate the results of U.S. elections.

24. Electronic voting machines and software manufactured by industry leaders, specifically including ES&S, are vulnerable to cyberattacks before, during, and after an election in a manner that could alter election outcomes.

25. These systems can be connected to the internet or cellular networks, which provides an access point for unauthorized manipulation of their software and data. They often rely on outdated versions of Windows, which lack necessary security updates. Both of these common shortcomings leave the systems vulnerable to generalized, widespread-effect attacks.

26. Industry leaders have compounded these vulnerabilities by consistently refusing to make their systems open to the public and subject to scientific analysis by objective experts to determine whether it is secure from manipulation or intrusion. This lack of transparency invites disastrous consequences.

27. Since 2000, alleged, attempted, and actual illegal manipulation of votes through electronic voting machines has apparently occurred on multiple occasions.

28. Expert testimony demonstrates that all safety measures intended to secure electronic voting machines against manipulation of votes, such as risk limiting audits and logic and accuracy tests, can be defeated.

Background: The History of Electronic Voting Systems

29. Prior to 2002, most states, including Alabama, conducted their elections overwhelmingly using secure, reliable, and auditable paper-based systems.

30. After the recount of the 2000 presidential election in Florida and the ensuing *Bush v. Gore* decision, Congress passed the Help America Vote Act in 2002.[1] In so doing, Congress opened the proverbial spigot. Billions of federal dollars were spent to move states, including Alabama, from paper-based voting systems to electronic, computer-based systems.

31. Since 2002, elections throughout the United States have increasingly and largely been conducted using a handful of computer-based election management systems. These systems are created, maintained, and administered by a small number of companies

[1] 52 U.S.C. § 20901 *et seq*.

having little to no transparency to the public, producing results that are far more difficult to audit than paper-based systems, and lack any meaningful federal standards or security requirements beyond what individual states may choose to certify. Leaders of both major parties have expressed concern about this lack of transparency, analysis and accountability.

32. In fact, experts and policymakers from across the political spectrum have raised glaring failures with electronic voting systems. just three months ago, a computer science expert in *Curling v. Raffensperger*, Case No. 1:17-cv-02989-AT (U.S. Dist. Ct., N.D. Ga.), identified catastrophic failures in electronic voting machines used in sixteen states, including Alabama. The expert testified that the failures include the ability to defeat all state safety procedures. This caused the Cybersecurity and Infrastructure Security Agency ("CISA") to enter an appearance and urge the federal district court to not allow disclosure of the expert's report detailing these failures. The district court refused to allow disclosure of that expert report to date. Secrecy destroys public confidence in our elections and election systems that result in secrecy undermine our democratic process.

33. The problems with the electronic voting systems are not only technical, but structural. To date, only three companies collectively provide voting machines and software for 90% of all eligible voters in the United States. Most of those machines are over a decade old, have critical components manufactured overseas in countries, some of which are hostile to the United States, and use software that is woefully outdated and vulnerable to catastrophic cyberattacks. Indeed, countries like France have banned the use of electronic voting machines due to lack of security and related vulnerabilities.

34. Given the limitations and flaws of existing technology, electronic voting machines cannot legally be used to administer elections today and for the foreseeable future, unless and until their current electronic voting system is objectively validated.

35. As of 2019, ES&S, Dominion, and Hart InterCivic supplied more than ninety percent of the nationwide "voting machine market."[2] ES&S controls even more than that share of the market in Alabama. All three of these providers' electronic voting machines can be hacked or compromised with malware, as has been demonstrated by recognized computer science experts, including experts from the University of Michigan, Princeton University, Georgetown University, and other institutions and presented to various congressional committees. All can be, and at various steps in the voting, counting, tabulating, and/or reporting process are designed to be, connected to the internet or cellular networks, directly or indirectly.

36. This small cadre of companies supplies the hardware and software for the electronic voting machines, in some cases manages the voter registration rolls, maintains the voter records, partially manages the elections, programs the vote counting, and reports the election results.

37. Jurisdictions throughout the nation, including Alabama, have functionally outsourced all election operations to these private companies. In the upcoming 2022

[2] Pam Fessler & Johnny Kauffman, *Trips to Vegas and Chocolate-Covered Pretzels: Election Vendors Come Under Scrutiny*, NPR (May 2, 2019) (https://www.npr.org/2019/05/02/718270183/trips-to-vegas-and-chocolate-covered-pretzels-election-vendors-come-under-scruti).

Election, over three thousand counties across the United States will have delegated the governmental responsibility for programming and administering elections to private contractors.

38. This includes all counties in Alabama, most of which have contracted with ES&S to provide machines, software, and services for the 2022 Election.

39. By its own account, ES&S is a "one-stop shop of integrated solutions for every step of the election cycle."[3] ES&S offers its services "before," "during," and "after" an election, which include:

Before the election:

- Voter registration
- Ballot layout
- Ballot Printing
- Tabulator Programming
- Poll worker training

During the election:

- Electronic pollbooks
- Vote-by-mail
- ADA ballots
- Central tabulation
- Precinct paper tabulation

[3] https://www.essvote.com/how-we-help/ (Visited May 3, 2022).

After the election

- Customer help desk
- Data collection
- Results reporting
- Technical support
- Canvassing
- Auditing
- Recounts[4]

40. ES&S, in its normal course of business, including the 2022 Election in Alabama, manufactures, distributes, and maintains voting hardware and software. Dominion also executes software updates, fixes, and patches for its voting machines and election management systems.

41. After votes are tabulated at the county level using ES&S's electronic election management system in the 2022 Election, the vote tallies will be uploaded over the internet to an election reporting system.

42. ES&S's machines and systems range from the "Ballot on Demand"—software that creates the ballots voters will mark while voting, as well as programing the tabulators of those votes—to its "ExpressVote" devices on which voters mark their votes ("ballot marking devices," or "BMDs"), to the machines that tabulate the votes at the precinct level, to the machines that receive and tabulate the various precinct results

[4] *Id.*

("centralized tabulation"), to the systems and options for transmitting those results from the BMD to the precinct tabulator to the central tabulator to, ultimately, the official government authority responsible for certifying the election results. In the 2022 Election, many Alabamans will cast their votes on ES&S BMDs, while nearly *all* Alabamans will have their votes tabulated with ES&S machines.

43. ES&S controls the administration and conduct of the elections in those jurisdictions where its systems are deployed, including Alabama. Any vulnerabilities or weaknesses in ES&S's systems, at the very least, call into question the integrity and reliability of all election results coming from those jurisdictions. ES&S has refused to disclose its software and other parts of its electronic voting systemin order to subject it to neutral expert evaluation.

Decades of Evidence Prove Electronic Voting Systems Do Not Provide a Secure, Transparent, or Reliable Vote

44. Over the last two decades the United States has transitioned from a safe, secure, auditable paper-based system to an inherently vulnerable, network-exposed electronic equipment-based system. The transition to increased reliance on electronic systems and computer technology has created unjustified new risks of hacking, election tampering, and electronic voting fraud.

45. With each passing election the unreliability of electronic voting machines has become more apparent. In light of this experience, the vote tallies reported by electronic voting machines cannot, without objective evaluation, be trusted to accurately show which candidates actually received the most votes.

46. Credible allegations of electronic voting machine "glitches" that materially impacted specific races began to emerge in 2002. *Black Box Voting*, the seminal publication documenting early pitfalls of electronic voting systems, chronicles the following failures:

> In the Alabama 2002 general election, machines made by Election Systems and Software (ES&S) flipped the governor's race. Six thousand three hundred Baldwin County electronic votes mysteriously disappeared after the polls had closed and everyone had gone home. Democrat Don Siegelman's victory was handed to Republican Bob Riley, and the recount Siegelman requested was denied. Six months after the election, the vendor shrugged. "Something happened. I don't have enough intelligence to say exactly what," said Mark Kelley of ES&S.
>
> […]
>
> In the 2002 general election, a computer miscount overturned the House District 11 result in Wayne County, North Carolina. Incorrect programming caused machines to skip several thousand party-line votes, both Republican and Democratic. Fixing the error turned up 5,500 more votes and reversed the election for state representative.
>
> […]
>
> Voting machines failed to tally "yes" votes on the 2002 school bond issue in Gretna, Nebraska. This error gave the false impression that the measure had failed miserably, but it actually passed by a 2 to 1 margin. Responsibility for the errors was attributed to ES&S, the Omaha company that had provided the ballots and the machines.
>
> […]
>
> In the November 2002 general election in Scurry County, Texas, poll workers got suspicious about a landslide victory for two Republican commissioner candidates. Told that a "bad chip" was to blame, they had a new computer chip flown in and also counted the votes by hand — and found out that Democrats actually had won by wide margins, overturning the election.[5]

[5] Available at https://blackboxvoting.org/black-box-voting-book/.

47. By 2004, explicit evidence that electronic voting machines were susceptible to intentional manipulation, and that malicious actors sought to exploit this vulnerability, became public. In that year, cyber expert Clint Curtis testified under oath before the House Judiciary Committee that he had previously been hired to create a program that would change the results of an election without leaving any trace of the change. He claimed he wrote this program with ease. Mr. Curtis' testimony can be watched here: https://www.youtube.com/watch?v=JEzY2tnwExs.

48. During the next election cycle, in 2006, a team of computer scientists at Princeton University analyzed the Diebold AccuVote-TS voting machine, then one of the most widely-deployed electronic voting platforms in the United States. They found, "Malicious software running on a single voting machine can steal votes with little risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss. . . . Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute. . . . AccuVote-TS machines are susceptible to voting machine viruses – computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre- and post-election activity." The Princeton team prepared a video demonstration showing how malware could flip votes. In the video, mock election votes were cast in favor of George Washington by a 4 to 1 margin, but the paper print-out that reported the results showed Benedict Arnold prevailing by a margin of 3 to 2. Malicious vote-stealing malware was the

sole reason for reallocation of votes. The malware deleted itself after the election, leaving no evidence that the voting machine was ever hijacked or any votes stolen.

49. In 2009 Diebold sold (at a loss) "Premier," its electronic voting systems business unit, which by then was known for its technical problems and unreliable security and accuracy. The Premier intellectual property passed (from ES&S) to Dominion in May 2010. That intellectual property included the GEMS election management system software. Dominion quickly incorporated GEMS into its own products and by 2011 was selling election equipment that had updated GEMS software at its heart. But GEMS was notorious for being, according to Harper's Magazine, "a vote rigger's dream" that "could be hacked, remotely or on-site, using any off-the-shelf version of Microsoft Access, and password protection was missing for supervisor function." Lack of encryption on its audit logs "allowed any trace of vote rigging to be wiped from the record." Computer scientists from Johns Hopkins University and Rice University found GEMS "far below even the most minimal security standards applicable in other contexts" and "unsuitable for use in a general election."

50. In 2015 the Brennan Center for Justice issued a report listing two and a half-pages of instances of issues with voting machines, including a 2014 investigation which found "voters in Virginia Beach observed that when they selected one candidate, the machine would register their selection for a different candidate."[6] The investigation also

[6] Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, p.13 (Sep. 15, 2014) (available at https://www.brennancenter.org/our-work/research-reports/americas-voting-machines-

found that the Advanced Voting Solutions WINVote machine, which is Wi-Fi-enabled, "had serious security vulnerabilities" because wireless cards on the system could allow "an external party to access the [machine] and modify the data [on the machine] without notice from a nearby location," and "an attacker could join the wireless ad-hoc network, record voting data or inject malicious [data.]"

51. In 2016, following in the footsteps of the Johns Hopkins, Rice, and 2006 Princeton teams, Princeton Professor of Computer Science Andrew Appel told an interviewer how he had purchased a voting machine for $82 on the internet – the Sequoia AVC Advantage, still set to be used in the 2016 election in a number of states – and replaced the machine's ROM chips in mere minutes using little more than a screwdriver, thereby "throw[ing] off the machine's results, subtly altering the tally of votes, never to betray a hint to the voter."[7]

risk).

[7] Ben Wofford, *How to Hack an Election in 7 Minutes*, Politico (Aug. 5, 2016) (https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144/).

52. During that 2016 election cycle evidence emerged of foreign state actors seeking to affect U.S. voting. "Russian agents probed voting systems in all 50 states, and successfully breached the voter registration systems of Alabama and Illinois."[8] The Robert Mueller report and an indictment of twelve Russian agents later confirmed that Russian hackers had targeted vendors that provide election software, and Russian intelligence 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."[9]

[8] Jordan Wilkie, *'They think they are above the law': the firms that own America's voting system*, The Guardian (Apr. 23, 2019) (https://www.theguardian.com/us-news/2019/apr/22/us-voting-machine-private-companies-voter-registration).
[9] Robert S. Mueller, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, vol. 1, p. 51 (Mar. 2019). (https://www.justice.gov/archives/sco/file/1373816/download).

53. After these revelations about the 2016 election, Jake Braun, a former security advisor for the Obama administration and organizer of the DEFCON Hacking Conference was asked in 2017, "Do you believe that right now, we are in a position where the 2020 election will be hacked?" He answered, "Oh, without question. I mean the 2020 election will be hacked no matter what we do."

54. Following a 2017 runoff election in a Georgia congressional race, an advocacy organization and individual voters filed suit in federal district court seeking to set aside the results. They alleged the election "took place in an environment in which sophisticated hackers – whether Russian or otherwise – had the capability and intent to manipulate elections in the United States" and had "easy access" to do so.

55. The Georgia plaintiffs supported their allegations with expert testimony from Logan Lamb, who testified that he freely accessed official Georgia state election files hosted on an "elections.kennesaw.edu" server, including voter histories and personal information of all Georgia voters; tabulation and memory card programming databases for past and future elections; instructions and passwords for voting equipment administration; and executable programs controlling essential election resources. Lamb stated that these sensitive 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. Lamb said the publicly accessible files created and maintained on this server were used to program virtually all other voting and tabulation equipment used in Georgia's elections.

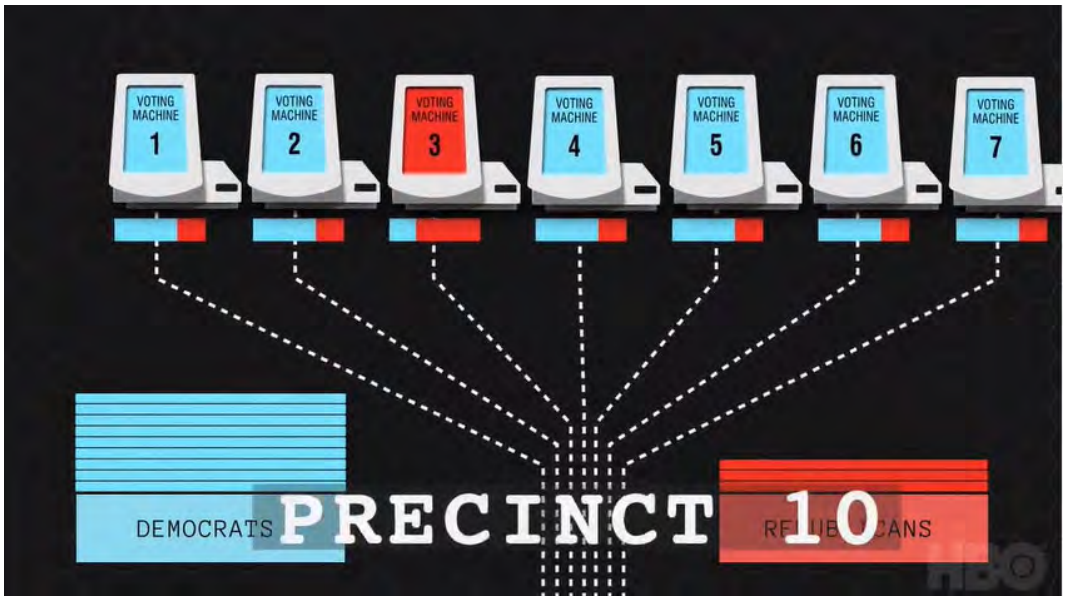
56. In 2019 a group of election security experts found "nearly three dozen backend election systems in 10 states connected to the internet over the last year," including

in "critical swing states" Wisconsin, Michigan, and Florida. Some of the jurisdictions "were not aware that their systems were online" and were "publicly saying that their systems were never connected to the internet because they didn't know differently."[10] The Associated Press reported that the vast majority of 10,000 election jurisdictions nationwide were still using Windows 7 or older operating systems to create ballots, program voting machines, tally votes, and report counts, which was a problem because "Windows 7 reaches its 'end of life' on Jan. 14 [2020], meaning Microsoft stops providing technical support and producing "patches" to fix software vulnerabilities, which hackers can exploit."[11]

57. In March 2020, the documentary *Kill Chain: The Cyber War on America's Elections* detailed the vulnerability of electronic voting machines. In the film, Hursti showed that he hacked digital election equipment to change votes back in 2005, and said the same machine that he hacked in 2005 was slated for use in 20 states for the 2020 election. *Kill Chain* also included facts about a Georgia election in which one machine out of seven in a precinct registered a heavy majority of Republican votes, while every other machine in the precinct registered a heavy majority of Democratic votes. Dr. Kellie

[10] Kim Zetter, *Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials*, Vice (Aug. 8, 2019) (https://www.vice.com/en/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials).
[11] Tami Abdollah, *New election systems use vulnerable software*, Associated Press (July 13, 2019) (https://apnews.com/article/operating-systems-ap-top-news-voting-voting-machines-pennsylvania-e5e070c31f3c497fa9e6875f426ccde1).

Ottoboni, Department of Statistics, UC Berkeley, stated the likelihood of this happening by chance was less than one in a million.[12]



Electronic Voting Systems Manufacturers Source and Assemble Their Components in Hostile Nations

58. Electronic voting machines are also vulnerable to malicious manipulation through illicit software installed on their component parts during the manufacturing process. The Congressional Task Force on Election Security's Final Report in January 2018 stated, "many jurisdictions are using voting machines that are highly vulnerable to an outside attack," in part because "many machines have foreign-made internal parts." Therefore, "'[A] hacker's point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line.'"[13]

[12] Screenshot from https://www.facebook.com/KillChainDoc/videos/2715244992032273/.
[13] CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT at 25 (2018) (https://homeland.house.gov/imo/media/doc/TFESReport.pdf).

59. Computer server security breaches as a result of hardware manufactured in China have been discovered by the U.S. Department of Defense (2010), Intel Corp. (2014), an FBI investigation that affected multiple companies (2015), and a government contractor providing intelligence services (2018).[14]

60. Leading electronic voting machine manufacturers source many parts from China, Taiwan, and the Philippines.[15]

State and Federal Lawmakers from Both Parties Have Long Been Aware of the Problems with Electronic Voting Systems

61. As the years passed and the evidence mounted, lawmakers and officials throughout the nation have realized these problems with electronic voting machines cannot be ignored.

62. The Congressional Task Force on Election Security issued a Final Report in January 2018 that identified the vulnerability of U.S. elections to foreign interference:[16] "According to DHS, Russian agents targeted election systems in at least 21 states, stealing personal voter records and positioning themselves to carry out future attacks. . . media also reported that the Russians accessed at least one U.S. voting software supplier . . . in most

---

[14] Jordan Robertson and Michael Riley, *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, Bloomberg (October 4, 2018). (https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies).

[15] Ben Popken, Cynthia McFadden and Kevin Monahan, *Chinese parts, hidden ownership, growing scrutiny: Inside America's biggest maker of voting machines*, NBC News (Dec. 19, 2019) (https://www.nbcnews.com/news/all/chinese-parts-hidden-ownership-growing-scrutiny-inside-america-s-biggest-n1104516).

[16] CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT (2018) (https://homeland.house.gov/imo/media/doc/TFESReport.pdf).

of the targeted states officials saw only preparations for hacking . . . [but] in Alabama and Illinois, voter registration databases were reportedly breached. . . If 2016 was all about preparation, what more can they do and when will they strike? . . . [W]hen asked in March about the prospects for future interference by Russia, then-FBI Director James Comey testified before Congress that: '[T]hey'll be back. They'll be back in 2020. They may be back in 2018.'"[17]

63. In a March 21, 2018 hearing held by the Senate Intelligence Committee relating to potential foreign interference in the 2016 election, Senator Ron Wyden warned that:

> Forty-three percent of American voters use voting machines that researchers have found have serious security flaws including backdoors. These companies are accountable to no one. They won't answer basic questions about their cyber security practices and the biggest companies won't answer any questions at all. Five states have no paper trail and that means there is no way to prove the numbers the voting machines put out are legitimate. So much for cyber-security 101… The biggest seller of voting machines is doing something that violates cyber-security 101, directing that you install remote-access software which would make a machine like that a magnet for fraudsters and hackers.

64. Senator Wyden did not see his concerns addressed. On December 6, 2019, he, along with his Democratic colleagues in Congress – Senator Elizabeth Warren, Senator Amy Klobuchar, and Congressman Mark Pocan – published an open letter concerning major voting system manufacturers. In the letter, they identified numerous problems:

- "trouble-plagued companies" responsible for manufacturing and maintaining voting machines and other election administration

[17] *Id*. at 6-7.

equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems."

- "the election technology industry has become highly concentrated ... Today, three large vendors – Election Systems & Software, Dominion, and Hart InterCivic – collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States."

- "Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. . . . voting machines are reportedly falling apart, across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk. . . . Moreover, even when state and local officials work on replacing antiquated machines, many continue to 'run on old software that will soon be outdated and more vulnerable to hackers.'"

- "[J]urisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems-leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.[]"

65. Senator Warren, on her website, identified an additional problem: "These vendors make little to no information publicly available on how much money they dedicate to research and development, or to maintenance of their voting systems and technology. They also share little or no information regarding annual profits or executive compensation for their owners."

66. During a Senate Judiciary Committee hearing in June 2018, then-Senator Kamala Harris warned that, in a demonstration for lawmakers at the Capitol, election machines were "hacked" before the lawmakers' eyes. Two months later, Senator Klobuchar stated on national television, "I'm very concerned you could have a hack that

finally went through. You have 21 states that were hacked into, they didn't find out about it for a year."

67. While chairing the House Committee on Homeland Security in July of 2018, Republican Congressman Michael McCaul decried, "Our democratic system and critical infrastructures are under attack. In 2016, Russia meddled in our Presidential election through a series of cyber attacks and information warfare. Their goals were to undermine the credibility of the outcome and sow discord and chaos among the American people…."

68. Senator Wyden stated in an interview, "[T]oday, you can have a voting machine with an open connection to the internet, which is the equivalent of stashing American ballots in the Kremlin. . . . [As] of today, what we see in terms of foreign interference in 2020 is going to make 2016 look like small potatoes. This is a national security issue! . . . The total lack of cybersecurity standards is especially troubling . . . But the lack of cybersecurity standards leads local officials to unwittingly buy overpriced, insecure junk. Insecure junk guarantees three things: a big payday for the election-tech companies, long lines on Election Day, and other hostile foreign governments can influence the outcome of elections through hacks."

69. In March of 2022, White House press secretary Jen Psaki said the Russian government in 2016 "hacked our election here" in the United States.

70. The following month, Dara Lindenbaum, a nominee to serve on the Federal Election Commission, testified before the Senate Rules and Administration Committee. Lindenbaum was asked about her role as an election lawyer representing Stacey Abrams's campaign for governor of Georgia in 2018. Lindenbaum acknowledged she had alleged

voting machines were used to illegally switch votes from one candidate to another during the 2018 election in Georgia. [18]

Electronic Voting Machine Companies Have Not Been Transparent Concerning Their Systems

71. Election officials and voting system manufacturers have publicly denied that their election equipment is connected to the internet in order to assert the equipment is not susceptible to attack via a networked system.[19]

72. Prior to 2020, ES&S had represented to its customers and potential customers that its DS200 voting system was "fully certified and compliant with EAC guidelines" even if used with a modem—a critical access point by which unauthorized access can be made. In a letter dated March 20, 2020, EAC issued a letter to ES&S stating that ES&S had misrepresented that its voting machines with modems were EAC compliant. The EAC ordered ES&S to take corrective actions, including to:

- Revise ES&S's marketing material to properly represent voting systems that have been certified by the EAC.
- Provide the EAC with a plan to removal all misrepresented marketing material from circulation.

---

[18] PN1758 — Dara Lindenbaum — Federal Election Commission, https://www.congress.gov/nomination/117th-congress/1758; https://www.youtube.com/watch?v=wCPLL_D_spc E**rror! Hyperlink reference not valid.**

[19] Kim Zetter, *Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials*, Vice (Aug. 8, 2019) (https://www.vice.com/en/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials).

- Notify ES&S's customers and potential customers that previous information was inaccurate.
- Provide customers and potential customers with corrected information.

73. The admonishment from the EAC went unreported for nearly five months. When POLITICO finally obtained a copy of the EAC's letter in August of 2020, POLITICO noted that ES&S "has previously said that more than 33,000 DS200 optical scan machines with modems are in use in 11 states and the District of Columbia but has never identified which jurisdictions this includes beyond D.C."[20]

74. Despite its public admonition of ES&S, it would turn out that the EAC had held a series of weekly closed-door meetings with manufacturers of electronic voting systems between July and August of 2020. Following these sessions, the EAC approved changes to its Voluntary Voting System Guidelines that do not comply with federal law, specifically the Help America Vote Act of 2002, 52 U.S.C. § 20901 *et seq*.

75. The approved changes served to reduce the cost to manufacturers, while substantially weakening the security of voting systems. Despite tens of thousands of public comments and the recommendations of security experts, the EAC has refused to institute a complete ban on wireless modems in its voting systems.[21]

---

[20] Kim Zetter, *Election Commission Orders Top Voting Machine Vendor to Correct Misleading Claims*, POLITICO (Aug. 13, 2020) (https://www.politico.com/news/2020/08/13/election-voting-machine-misleading-claims-394891).

[21] *Commissioner Hovland Statement to the TGDC Regarding VVSG 2.0 Principle and Guidelines Public Comments* (Jan. 15, 2020), https://www.eac.gov/sites/default/files/2020-02/Commissioner_Hovland_Statement_to_the_TGDC_Regarding_VVSG_2.pdf (acknowledging

76. In the 2022 Election, voting precincts in Alabama will rely on the DS200 machines.[22] Thanks to the largely successful efforts of ES&S and its industry cohorts to conceal information about its products, it is not possible to determine which of these machines may have wireless capabilities throughout the 2022 Election.

77. What is more, ES&S has been caught in lies about its equipment before. In 2018, Vice reported that ES&S falsely denied selling voting machines with remote access software, a fact ES&S later admitted was true in a letter to Senator Ron Wyden (D. Or.).[23]

78. John Poulous, the CEO of Dominion Voting Systems, testified in December 2020 that Dominion's election systems are "closed systems that are not networked meaning they are not connected to the internet." This is false.

79. In a May 2016 interview, Dominion Vice President Goran Obradovic stated, "All devices of the ImageCast series have additional options such as modems for wireless and wired transfer of results from the very polling place…."[24] During the 2020 election Dominion election equipment was connected to the internet when it should not have been.[25]

---

receipt of tens of thousands of comments advocating to "ban wireless; require hand-marked paper ballots").

[22] https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2022/state/1

[23] Kim Zetter, *Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States*, Vice (July 17, 2018) (https://www.vice.com/en/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states).

[24] Economy & Business, Interview: How do the others do this? A technological solution exists for elections with complete security, privacy, and transparency pp.30, 31 (May 2016) (https://ekonomijaibiznis.mk/ControlPanel/Upload/Free_Editions/wZ0X5bz60KCgpcvFcEBvA/maj%202016%20ENG/mobile/index.html#p=31).

[25] Aff. of Patrick J. Colbeck, *Costantino v. City of Detroit*, no. 20-014780-AW (Wayne

A Dominion representative in Wayne County, Michigan stated that during the voting in the 2020 election there were irregularities with Dominion's election equipment, including that equipment was connected to the internet and equipment had scanning issues.

80. On Monday, November 2, 2020, the day before the 2020 election, Dominion uploaded software updates into election equipment that Dominion had supplied in the United States.[26] These software updates were unplanned and unannounced. In some counties in Georgia, Dominion's software update caused election equipment to malfunction the next day during the election. The supervisor of one County Board of Elections stated that Dominion "uploaded something last night, which is not normal, and it caused a glitch," and "[t]hat is something that they don't ever do. I've never seen them update anything the day before the election." Dominion had earlier publicly denied that any updates just prior to election day were made and that its election equipment was connected to the internet—both of which were false statements.[27]

81. In December 2020, the Department of Homeland Security's Cybersecurity & Infrastructure Agency ("CISA") revealed that malicious hackers had compromised and exploited SolarWinds Orion network management software products.[28] On April 15, 2021,

---

Co., Mich. Cir. Ct. Nov. 8, 2020).

[26] Kim Zetter, *Cause of Election Day Glitch in Georgia Counties Still Unexplained*, Politico (Nov. 12, 2020) (https://www.politico.com/news/2020/11/04/georgia-election-machine-glitch-434065).

[27] Isabel van Brugen, *Dominion Voting Machines Were Updated Before Election, Georgia Official Confirms*, The Epoch Times (Dec. 4, 2020) (https://www.theepochtimes.com/dominion-voting-machines-were-updated-before-election-georgia-official-confirms_3604668.html).

[28] CISA, *CISA issues emergency directive to mitigate the compromise of SolarWinds Orion network management products* (Dec. 14, 2020) (https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network).

the White House announced imposition of sanctions on Russia in response to Russian "malicious cyber activities, such as the SolarWinds incident."[29]

82. Dominion CEO John Poulos stated that Dominion did not use SolarWinds.

83. Dominion in fact did use SolarWinds. Dominion's website formerly displayed a SolarWinds logo, but that logo was removed.

84. Dominion refuses to provide access to allow the public to forensically investigate its "proprietary" software, machines, and systems, to determine whether its election equipment is secure, has been hacked, or has malware installed.

85. No electronic voting system to be used in Alabama in the 2022 Election employs "open source" technology, which is electronic equipment for which the details of the components of the system, including its software, is published and publicly accessible. Though Dominion and E&S do not offer open source voting technology, it has been available to Defendants from other vendors for years.

86. Defendants have failed or refused to institute open source voting technologies in Alabama, even though such technology would promote both security and transparency, as voters and office-seekers throughout Alabama would know the specific risks to, or manipulation of, election results.

[29] The White House, *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government* (Apr. 15, 2021) (https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/).

87. This lack of transparency by electronic voting machine companies has created a "black box" system of voting which lacks credibility and integrity.

Irregularities and Evidence of Illegal Vote Manipulations in Electronic Voting Systems During the 2020 General Election Have Been Found

88. Evidence has been found of illegal vote manipulation on electronic voting machines during the 2020 election.

89. Dominion Democracy Suite software was used to tabulate votes in 62 Colorado counties, including Mesa County, during the 2020 election. Subsequent examination of equipment from Mesa County showed the Democracy Suite software created unauthorized databases on the hard drive of the election management system servers. On March 21, 2022, electronic database expert Jeffrey O'Donnell and computer science expert Dr. Walter Daugherity published a report concluding that ballots were manipulated in the unauthorized databases on the Mesa County server during Colorado's November 2020 and April 2021 elections.

90. On February 28, 2022, and after a comprehensive review of the Dominion systems used in Colorado, cybersecurity expert Douglas Gould published a report concluding that the system was "configured to automatically overwrite log files that exceed 20 MB, thereby violating federal standards that require the preservation of log files," that it was configured "to allow any IP address in the world to access the SQL service port, (1433), which violates 2002 VSS security standards," and that it "uses generic user IDs and passwords and a common shared password, some of which have administrative access," in violation of 2002 VSS security standards.

91. Electronic forensic experts examined equipment used in Michigan to administer voting during the 2020 election and concluded the equipment had been connected to the internet, either by Wi-Fi or a LAN wire, that there were multiple ways the election results could have been modified without leaving a trace; and the same problems have been around for 10 years or more. One expert "examined the forensic image of a Dominion ICX system utilized in the November 2020 election and discovered evidence of internet communications to a number of public and private IP addresses."

92. In Wisconsin, during the voting in the 2020 election, Dominion election equipment that was not supposed to be connected to the internet was connected to a "hidden" Wi-Fi network.[30]

93. In April 2021, the Biden administration announced sanctions against Russia for election interference and hacking in the 2020 United States presidential election.[31]

94. Following the 2020 election, lawmakers in multiple states initiated investigations and audits of the results.

95. The Arizona Senate hired a team of forensic auditors to review Maricopa County's election process. The auditors issued a partial audit report on September 24, 2021, which found: (1) "None of the various systems related to elections had numbers that would balance and agree with each other. In some cases, these differences were significant"; (2)

[30] M.D. Kittle, *Emails: Green Bay's 'Hidden' Election Networks*, Wisconsin Spotlight (Mar. 21, 2021) (https://wisconsinspotlight.com/emails-green-bays-hidden-election-networks/).
[31] Natasha Truak and Amanda Macias, *Biden administration slaps new sanctions on Russia for cyberattacks, election interference*, CNBC (Apr. 16, 2021) (https://www.cnbc.com/2021/04/15/biden-administration-sanctions-russia-for-cyber-attacks-election-interference.html).

"Files were missing from the Election Management System (EMS) Server"; (3) "Logs appeared to be intentionally rolled over, and all the data in the database related to the 2020 General Election had been fully cleared"; (4) "Software and patch protocols were not followed"; and (5) basic cyber security best practices and guidelines from the CISA were not followed.[32]

96. Retired Wisconsin Supreme Court Justice Michael Gableman conducted an investigation of the 2020 election in Wisconsin at the direction of the Wisconsin Assembly. Gableman issued a report in March 2022 noting that "at least some machines had access to the internet on election night."[33] He concluded that several machines manufactured by ES&S and used in the 2020 election in Wisconsin were "made with a 4G wireless modem installed, enabling them to connect to the internet through a Wi-Fi hotspot."

97. During a December 30, 2020 live-streamed hearing held by the Georgia Senate Judiciary Subcommittee on Elections, an expert witness testified that an active Dominion polling pad had been hacked and the intrusion was being maintained even as he was speaking.[34]

---

[32] *Maricopa County Forensic Election Audit, Volume I*, pp.1-3 (Sept. 24, 2021) (available at https://c692f527-da75-4c86-b5d1-8b3d5d4d5b43.filesusr.com/ugd/2f3470_a91b5cd3655445b498f9acc63db35afd.pdf).
[33] Office of the Special Counsel: Second Interim Investigative Report On the Apparatus & Procedures of the Wisconsin Elections System, March 1, 2022, p. 13.
[34] Hearing of Georgia Senate Judiciary Subcommittee on Elections, Dec. 30, 2020 (https://www.youtube.com/watch?v=D5c034r0RlU beginning at 4:07:58).

Despite these Alarming Problems, Defendants Intend to Allow Electronic Voting Systems to be Used in the 2022 Election

98. Alabama allows for electronic voting systems, provided they meet certain requirements. Ala. Code § 17-2-4.

99. Alabama law specifically provides that "no electronic vote counting system shall be used unless it has been constructed so that it[…]

> (2) Permits each elector to vote at any election for all persons and offices for whom and for which he or she is lawfully entitled to vote; to vote for as many persons for an office as he or she is entitled to vote for; and to vote for or against any question upon which he or she is entitled to vote.
>
> […]
>
> (5) Is capable of correctly counting votes.
>
> […]
>
> (12) Is capable of accurately and correctly tabulating each vote and having the same so certified.
>
> Ala. Code § 17-7-21

100. Defendant Merrill and the Committee Defendants have allowed the voting machines to be currently certified for use in the State of Alabama: Elections Systems and Software (ES&S) M100 Precinct Counter, ES&S DS200, ES&S 450, ES&S DS850, Automark A100, A200, and A300, and ExpressVote 1.0 and 2.0."[35]

[35] https://www.sos.alabama.gov/newsroom/secretary-state-john-h-merrill-confirms-dominion-voting-systems-not-certified-use-alabama

101. Alabama intends to rely on electronic voting systems to record some votes and to tabulate nearly all votes cast in the State of Alabama in the 2022 Election, without disclosing the systems and subjecting them to neutral, expert analysis.[36]

102. Alabama's electronic election infrastructure is susceptible to malicious manipulation that can cause incorrect counting of votes. Despite a nationwide bipartisan consensus on this risk, election officials in Alabama continue to administer elections dependent upon unreliable, insecure electronic voting systems. These officials refuse to take necessary action to address known and currently unknown election security vulnerabilities, and in some cases have obstructed court authorized inspections of their electronic voting systems.

103. Plaintiffs seek the intervention of this Court because the Secretary of State and county officials throughout the State have failed to take constitutionally necessary measures to protect voters' rights to a secure and accurately counted election process. The State of Alabama and its officials bear a legal, constitutional, fiduciary and ethical duty and obligation to secure the State's electoral system, but they lack the will to do so.

104. In his official capacity, Merrill is the chief election officer for the State of Alabama. Defendant Merrill is responsible for the orderly and accurate administration of public election processes in the state of Alabama.

[36] https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2022/state/4

105. The Committee Defendants are charged with the duty "to ensure the examination and certification of electronic vote counting systems in the following manner:

> (1) By publicly examining all makes of electronic vote counting systems submitted and certifying whether such systems comply with the requirements of this section.
>
> (2) By inviting any vendor or company interested in selling an electronic vote counting system in Alabama to submit such equipment for examination. The vote counting system shall be certified after a satisfactory evaluation and testing has been performed to determine that the equipment meets the requirements of this article and performance and test standards for electronic voting systems issued by the Federal Election Commission. The committee may use certification of the equipment by an authorized independent testing authority, or successor entity, as evidence that the equipment meets the requirements of Section 17-7-21 and this section, where certification by the independent testing authority, or successor entity, is applicable. For the purpose of assisting in examining such system, the committee may employ not more than three individuals who are expert in one or more fields of data processing, mechanical engineering, and public administration, who may or may not be state employees and shall require from them a written report of their examination. The vendor submitting a system for certification shall pay to the State of Alabama by depositing with the State Treasury for distribution to reimburse the committee in an amount equal to the actual costs, if any, incurred in examining the system. Such reimbursement shall be made whether or not the system is certified. No member of the committee nor any examiner shall have any pecuniary interest in any voting equipment.
>
> (3) The committee shall approve only those electronic vote counting systems that are certified by an authorized independent testing authority, or successor entity, as meeting the performance and test standards for electronic voting systems issued by the Federal Election Commission.
>
> (4) After certification of any electronic vote counting system, the Secretary of State shall make and maintain a report on the system, and as soon as practicable shall send a notice of certification and, upon request, a copy of the report to all governing bodies of the counties of the state. Any electronic vote counting system that does not receive certification shall not be adopted or used at any election.
>
> (5) After an electronic vote counting system has been certified, any change or improvement in the system shall be certified by the committee prior to the

> adoption of such change or improvement by any county. The committee shall re-examine the electronic vote counting system to the extent necessary to determine that it, as changed or improved, is in compliance with the requirements of this article. If the system, as changed or improved, is not in compliance, the committee shall suspend all sales of the equipment or system in the state until such equipment or system complies with the requirements of this article.
>
> (6) The adoption of an electronic vote counting system in which votes are recorded on an electronic ballot as authorized in this article is hereby validated. It is the legislative intent of this subsection to declare that the use of electronic vote counting systems in which votes are recorded on an electronic ballot has, since the enactment of the Election Reform Act of 1983, been an acceptable method of electronic vote counting.

106. By allowing these electronic voting systems to be used in Alabama, all Defendants have failed to achieve the maximum degree of and impartiality of voting, counting, tabulating, and recording votes, by electronic vote counting systems.

107. Defendants intend to allow these failures to again occur in the 2022 Election.

Alabama's Voting Systems Do Not Comply with Alabama Law

108. Voting systems and voting equipment used in Alabama must

- Permit each elector to vote at any election for all persons and offices for whom and for which he or she is lawfully entitled to vote; to vote for as many persons for an office as he or she is entitled to vote for; and to vote for or against any question upon which he or she is entitled to vote.
- be capable of correctly counting votes; and
- be capable of accurately and correctly tabulating each vote and having the same so certified.

Ala. Code § 17-7-21

109. Electronic voting systems slated to be used in the 2022 Election, which are inaccurate and unreliable, do not meet these requirements.

Voting on Paper Ballots and Counting Those Votes by Hand Is the Most Effective and Presently the Only Secure Election Method

110. Plaintiffs seek for the Court to Order, an election conducted by paper ballot, as an alternative to the current framework. To satisfy constitutional requirements of reliability, accuracy, and security, the following is a summary of procedures that should be implemented:

- Ballots are cast by voters filling out paper ballots, by hand. The ballots are then placed in a sealed ballot box. Each ballot bears a discrete, unique identification number, which is made known by election officials only to the voter, so that the voter can later verify whether his or her ballot was counted properly. All ballots will be printed on specialized paper to confirm their authenticity.
- Though a uniform chain of custody, ballot boxes are conveyed to a precinct level counting location while still sealed.
- With party representatives, ballot boxes are unsealed, one at a time, and ballots are removed and counted in batches of 100, then returned to the ballot box. When all ballots in a ballot box have been counted, the box is resealed, with a copy of the batch tally sheets left inside the

box, and the batch tally sheets carried to the tally center with a uniform chain of custody.

- Ballots are counted, one at a time, by three independent counters, who each produce a tally sheet that is compared to the other tally sheets at the completion of each batch.
- At the tally center, two independent talliers add the counts from the batch sheets, and their results are compared to ensure accuracy.
- Vote counting from paper ballots is conducted in full view of multiple, recording, streaming cameras that ensure a) no ballot is ever touched or accessible to anyone off-camera or removed from view between acceptance of a cast ballot and completion of counting, b) all ballots, while being counted are in full view of a camera and are readable on the video, and c) batch tally sheets and precinct tally sheets are in full view of a camera while being filled out and are readable on the video.
- Each cast ballot, from the time of receipt by a sworn official from a verified, eligible elector, remains on video through the completion of precinct counting and reporting.
- The video be live-streamed for public access and archived for use as an auditable record, with public access to replay a copy of that auditable record.

- Anonymity will be maintained however, any elector will be able to identify their own ballot by the discrete, serial ballot number known only to themselves, and to see that their own ballot is accurately counted

111. Every county in Alabama, regardless of size, demographics, or any other ostensibly unique characteristic, can simply and securely count votes cast on paper ballots without using centralized machine-counting or computerized optical scanners.

112. The recent hand count in Maricopa County, the second largest voting jurisdiction in the United States, offers Defendant Merrill a proof-of-concept and a superior alternative to relying on corruptible electronic voting systems. Voting jurisdictions larger than any within Alabama, including France and Taiwan, have also proven that hand-count voting can deliver swift, secure, and accurate election results.

Past and Threatened Conduct of Defendant Merrill

113. Defendant Merrill is, in his capacity as Secretary of State and as the chief election officer of the State of Alabama, is responsible for ensuring the accuracy and integrity of all elections held in the state.

114. By certifying and allowing electronic voting systems to be used in prior elections in Alabama, Defendant Merrill has failed to meet these duties.

115. Defendant Merrill intends to commit these same violations up to and during the 2022 Election.

Past and Threatened Conduct of Committee Defendants

116. The Committee Defendants are charged with examining and approving all electronic voting equipment used in the State of Alabama.

117. It is further incumbent upon the Committee Defendants "to recommend procedures to be implemented by the Secretary of State under the Administrative Procedure Act where appropriate to achieve and maintain the maximum degree of correctness and impartiality of voting, counting, tabulating, and recording votes, by electronic vote counting systems." Ala. Code § 17-7-25(a).

118. The Committee Defendants have failed in their charge to achieve the maximum degree of correctness and impartiality throughout the State of Alabama in prior elections by failing to recommend procedures to the Secretary of State prohibiting the use of electronic voting systems.

119. The Committee Defendants intend to commit these same violations up to and during the 2022 Election.

Imminent Injury

120. Blanchard seeks the office of Governor of the State of Alabama.

121. To gain that office, Blanchard must prevail in the 2022 Election, in which all votes will be tabulated, and many votes will be cast, on electronic voting systems.

122. Blanchard intends to vote in the 2022 Election in Alabama. To do so, she will be required to cast her vote, and have her vote counted, through electronic voting systems.

123. Hanes seeks to retain his current office as a member of the Alabama House of Representatives.

124. To retain that office, Hanes must prevail in the 2022 Election, in which all votes will be tabulated, and many votes will be cast, on electronic voting systems.

125. All persons who vote in the 2022 Election, if required to vote using an electronic voting system or have their vote counted using an electronic voting system, will be irreparably harmed because the voting system does not reliably provide trustworthy and verifiable election results. The voting system therefore burdens and infringes their fundamental right to vote and have their vote accurately counted in conjunction with the accurate counting of all other legal votes, and *only* other legal votes.

126. Any voter who votes using a paper ballot will be irreparably harmed in the exercise of the fundamental right to vote if his or her vote is tabulated together with the votes of other voters who cast ballots using an unreliable, untrustworthy electronic system.

127. Any voter will be irreparably harmed in the exercise of the constitutional, fundamental right to vote if he or she is required to cast a ballot using – or in an election in which anyone will use – an electronic voting system, or if his or her ballot is tabulated using an electronic voting system.

128. Each of the foregoing harms to Plaintiffs is imminent for standing purposes because the 2022 Election is set to occur on a fixed date not later than eight months after the date when this action is to be filed.

129. No Plaintiff can be adequately compensated for these harms in an action at law for money damages brought after the fact because the violation of constitutional rights is an irreparable injury.

V. CLAIMS

COUNT I: VIOLATION OF DUE PROCESS

(*Seeking declaratory and injunctive relief against all Defendants*)

130. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

131. The right to vote is a fundamental right protected by Article I, § 6 of the Alabama Constitution.

132. The fundamental right to vote encompasses the right to have that vote counted accurately, and it is protected by the Due Process Clause of Article I, § 6 of the Alabama Constitution, as well as by Ala. Code §§ 17-2-4, 17-2-21, 17-2-23, and 17-2-25.

133. Defendants have violated Plaintiffs' fundamental right to vote by deploying an electronic voting equipment system that has:

(a) Failed to provide reasonable and adequate protection against the real and substantial threat of electronic and other intrusion and manipulation by individuals and entities without authorization to do so;

(b) Failed to include the minimal and legally required steps to ensure that such equipment could not be operated without authorization; to provide the minimal and legally required protection for such equipment to secure against unauthorized tampering; to test, inspect, and seal, as required by law, the equipment to ensure that each unit would count all votes cast and that no votes that were not properly cast

would not be counted; and to ensure that all such equipment, firmware, and software is reliable, accurate, and capable of secure operation as required by law;

(c) Failed to provide a reasonable and adequate method for voting by which Alabama electors' votes would be accurately counted.

134. By choosing to move forward in using an unsecure system, Defendants willfully and negligently abrogated their statutory duties and abused their discretion, subjecting voters to cast votes on an illegal and unreliable system--a system that must be presumed to be compromised and incapable of producing verifiable results.

135. Despite Defendants' knowledge that electronic voting systems used in Alabama do not comply and cannot be made to comply with state law, Defendants plan to continue to use these non-compliant systems in the 2022 Election.

136. Plaintiffs ask this Court to declare that these Defendants violated the Due Process Clause of Article I, § 6 of the Alabama Constitution; enjoin Defendants' use of electronic voting systems for future elections; and award attorneys' fees and costs for Defendants' causation of concrete injury to Plaintiffs, whose fundamental right to have their vote counted as cast was thwarted.

COUNT II: DECLARATORY JUDGMENT

(*Against All Defendants)*

137. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

138. Defendants' conduct will have the effect of violating the rights of the citizens of Alabama, as described above.

139. The Court has the authority pursuant to §§ 6-6-220 through 6-6-232 of the Code of Alabama and Rule 57 to issue an Order declaring that it is unlawful for the State of Alabama to conduct an election in which the votes are not accurately or securely tabulated.

140. If the State of Alabama is allowed to proceed with an election as described above, it will violate the rights of the citizens of the State by conducting an election with an unsecure, vulnerable electronic voting system which is susceptible to manipulation and intrusion.

141. Because of the above-described issues regarding the election system to be used by Defendants, the Court should issue an Order declaring that it is unconstitutional for the State to conduct an election which relies on the use of electronic voting systems to cast or tabulate the votes.

COUNT III: MANDAMUS

(*Seeking writ of mandamus against all Defendants*)

142. Plaintiffs incorporate and reallege all paragraphs in this Complaint.

143. If this Court does not grant Plaintiffs the declaratory or injunctive relief sought by this action, Plaintiffs seek a writ of mandamus from this Court, as there will be other adequate remedy at law.

144. Plaintiffs are entitled to vote and seek office in an election in which the fundamental right to vote is protected and in which all votes are accurately and securely tabulated.

145. By approving electronic voting systems for use in Alabama and intending for those systems to be used in the 2022 Election, Defendants have failed to uphold their statutory and constitutional duties to:

- Protect the fundamental right to vote;
- Achieve and maintain the maximum degree of correctness and impartiality of voting, counting, tabulating, and recording votes; and
- Ensure that vote counting systems used Alabama are only certified after a satisfactory evaluation and testing has been performed.

146. Unless and until this Court issues and order to Defendants to halt the use of electronic voting systems in the 2022 Election, Plaintiffs' constitutional and statutory rights will be violated.

147. This Court therefore must exercise its jurisdiction to issue a writ of mandamus ordering Defendants to prevent electronic voting systems from being used in the 2022 Election.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

1. Enter an Order finding and declaring it unconstitutional for any public election to be conducted using any model of electronic voting system to cast or tabulate votes, as set forth above.

2. Enter a preliminary and permanent injunction prohibiting Defendants from requiring or permitting voters to have votes cast or tabulated using, as set forth above,

compromised electronic voting systems, or in the alternative, issue a writ of mandamus ordering that Defendants prevent the use of any such electronic voting systems in the 2022 Election.

3. Enter an Order directing Defendants to conduct the 2022 Election consistent with the summary of procedures set forth in paragraph 110 of this Complaint.

4. Retain jurisdiction to ensure Defendants' ongoing compliance with the foregoing Orders.

5. Grant Plaintiff such other relief as the Court deems just and proper.

DATED: May 19, 2022

*/s/ Melissa L. Isaak*_____

Melissa L. Isaak (ISA 007)
The Isaak Law Firm
2815 Zelda Road
Suite B
Montgomery, AL. 36106
334-262-8200
Isaaklaw@gmail.com

Andrew D. Parker (MN Bar No.195042)
Parker Daniels Kibort, LLC
888 Colwell Building
123 N. Third Street
Minneapolis, MN 55401
Telephone: (612) 355-4100
Facsimile: (612) 355-4101
parker@parkerdk.com

Pro Hac Vice to be Filed

CERTIFICATION OF SERVICE ON ATTORNEY GENERAL

I HEREBY CERTIFY that a copy of this Complaint will be served on the Attorney General via Certified Mail, return receipt requested.

DATED: May 19, 2022

/s/ Melissa L. Isaak

Melissa L. Isaak (ISA 007)
The Isaak Law Firm
2815 Zelda Road
Suite B
Montgomery, AL. 36106
334-262-8200
Isaaklaw@gmail.com

Andrew D. Parker (MN Bar No.195042)
Parker Daniels Kibort, LLC
888 Colwell Building
123 N. Third Street
Minneapolis, MN 55401
Telephone: (612) 355-4100
Facsimile: (612) 355-4101
parker@parkerdk.com

Pro Hac Vice to be Filed