

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

**COALITION PLAINTIFFS' HEARING BRIEF ON EVIDENTIARY
PRESUMPTION ARISING FROM SPOILIATION OF EVIDENCE**

Introduction

In assessing Plaintiffs' likelihood of success on the merits, it is appropriate to consider the evidence that is likely to be produced in discovery and what that evidence is likely to establish. In 2018 this Court held Plaintiffs had carried their burden of showing likelihood of success on the merits and, as explained in other briefing, the evidence gathered and presented by Plaintiffs since has only enhanced their chances of success.

Plaintiffs have offered the unimpeached testimony of cybersecurity professional Logan Lamb—testimony verified by software and security engineer Chris Grayson—that the elections.kennesaw.edu server, a device that the State Defendants now argue is critical election infrastructure, was easily accessible to any

malicious actor who possessed even modest computer skills for at least six months. The State Defendants respond that there is no evidence that the extended exposure of the files on the Kennesaw server would have caused the election system any harm or increased the vulnerability of the already profoundly vulnerable system. The State Defendants' argument seems inconsistent with the dramatic descriptions of risk to the system they offered the Court in attempting to prevent Plaintiffs' access to the GEMS server in this matter—access that, unlike unauthorized access, would have been known to State, would have been pursuant to a protective order, and would have been under the supervision of the State and the Court. In short, the evidence strongly suggests that the State's amateurish protection of critical election infrastructure placed Georgia's election system at risk, and the State Defendants now appear to be desperate to cover-up the effects of their misfeasance—to the point of destroying evidence.

To the extent that any weight is given to the State's naked denials, however, the Court is authorized—if not compelled—to consider that the State wiped the server, knowingly destroying critical data, and then wiped a second server, both after being placed on notice of the pendency of this lawsuit. This brief details the facts of the spoliation of the elections.kennesaw.edu server *and* other relevant evidence and

outlines the law that would authorize appropriate presumptions and findings of culpability and wrongdoing on the part of the State.

This brief first outlines the controlling legal authorities, and then reviews the evidence relating to the spoliation of the KSU servers, massive numbers of memory cards, and the internal memory of the DREs themselves.

The Law of Spoliation

The law of spoliation is neither conceptually difficult to grasp in its application or its purpose. Spoliation sanctions are designed to deter litigants from destroying relevant evidence and to protect the integrity of the judicial process. *See Sentry Select Ins. Co. v. Treadwell*, 318 Ga. App. 844, 734 S.E.2d 818 (2012); *Wal-Mart Stores, Inc. v. Lee*, 290 Ga. App. 541, 659 S.E.2d 905 (2008).

The imposition of spoliation sanctions is governed by federal law, as spoliation is considered an evidentiary matter. *See Flury v. Daimler Chrysler Corp.*, 427 F.3d 939, 943 (11th Cir. 2005). Because federal law does not set forth specific spoliation guidelines, Georgia law informs the determination of the appropriateness of spoliation sanctions, citing five factors (which the Court noted were consistent with federal spoliation principles): “(1) whether the defendant was prejudiced as a result of the destruction of evidence; (2) whether the prejudice could be cured; (3) the practical importance of the evidence; (4) whether the plaintiff acted

in good or bad faith; and (5) the potential for abuse if expert testimony about the evidence was not excluded.” *Id.* at 495. *See also Kraft Reinsurance Ireland, Ltd. v. Palletts Acquisitions, LLC.*, 843 F. Supp. 1318, 1325 (N.D.Ga. 2011) (imposing sanctions for bad faith spoliation of evidence by defendant).

In December 2015, Rule 37 of the Federal Rules of Civil Procedure was amended to address the spoliation of electronically stored information. Rule 37(e) provides:

Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

- (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
- (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
 - (A) presume that the lost information was unfavorable to the party;
 - (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
 - (C) dismiss the action or enter a default judgment.

The Eleventh Circuit has not yet determined whether, with the 2015 amendment to Rule 37, the multi-factor test set forth in *Flury* is still applicable when

a party seeks sanctions based on the spoliation of electronically stored evidence. *See ML Healthcare Servs., LLC v. Publix Super Markets, Inc.*, 881 F.3d 1293, 1307–08 (11th Cir. 2018). Later district court decisions, however, continue to utilize the *Flury* test to analyze claims of spoliation. *See, e.g., Bland v. Sam's E., Inc.*, No. 4:17-CV-190 (CDL), 2019 WL 407406, at *1–2 (M.D. Ga. Jan. 31, 2019).

“In the Eleventh Circuit, ‘an adverse inference is drawn from a party's failure to preserve evidence only when the absence of that evidence is predicated on bad faith.’” *Mann v. Taser Int'l, Inc.*, 588 F.3d 1291, 1310 (11th Cir. 2009) (citation omitted) (holding mere negligence is insufficient to justify striking answer). A finding of bad faith does not require a finding of malice. “[M]alice may not always be required before a trial court determines that dismissal is appropriate...‘even when conduct is less culpable, dismissal may be necessary if the prejudice to the defendant is extraordinary, denying it the ability to adequately defend its case.’ Thus, in determining whether sanctions for spoliation are warranted, the trial court must weigh the degree of the spoliator's culpability against the prejudice to the opposing party.” *Bridgestone/Firestone N. Am. Tire, LLC v. Campbell*, 258 Ga. App. 767, 770, 574 S.E.2d 923, 927 (2002) (citation omitted). *See also Connor v. Sun Tr. Bank*, 546 F. Supp. 2d 1360, 1376 (N.D. Ga. 2008).

Here, the Court would be perfectly justified in finding malice and bad faith. Indeed, the facts scream “bad faith.” Almost immediately upon receiving notice of the pendency of this suit and allegations of the insecurity of electronic voting in the State, government officials and their agents with CES destroyed the evidence that was “ground zero” for establishing hacking, unauthorized access, and potential manipulation of election results. Within less than a day of the removal of this case to this court, the State and its agents destroyed a second server and all of its resident data. Such conduct would be incomprehensible absent one simple explanation: The State wished to eliminate evidence of exactly the kind of election manipulation Plaintiffs have alleged. And the spoliation has since continued, with the State deleting and overwriting data previously preserved in the DRE’s memories and on memory cards used in relevant elections.

The Threat

In August 2016, Logan Lamb, a cybersecurity professional was planning to meet with Merle King, the Executive Director of the Center for Elections Services (“CES”) housed at Kennesaw State University, to discuss a cyber-security research project. *See* Logan Lamb affidavit (“Lamb Aff.”), ¶ 2.¹ In preparation for that

¹ Mr. Lamb’s affidavit is attached hereto as Exhibit “A.”

meeting, Mr. Lamb visited the CES website to acquaint himself with the background of CES and Mr. King. *See* Lamb Aff., ¶ 3. Mr. Lamb was surprised to discover that he could use a script he spontaneously composed to access multiple gigabytes of information found on the website, including a voter registration database with personally identifiable information of voters, the GEMs database, and PDFs of election day supervisor passwords, among other data. *See* Lamb Aff., ¶ 4. Mr. Lamb also discovered that the CES servers were vulnerable to unauthorized users executing, creating, modifying, and deleting any data they chose to tamper with on the server. *See* Lamb Aff., ¶ 5. Mr. Lamb contacted Mr. King and advised him of those vulnerabilities. Mr. King assured Mr. Lamb the issues would be remediated. *See* Lamb Aff., ¶ 6.

In late February 2017, Mr. Lamb told a colleague, Chris Grayson, about the CES vulnerabilities. Mr. Grayson also visited the website and discovered that the vulnerabilities had not been remedied. *See* Lamb Aff., ¶ 7. Instead, Mr. Grayson was capable of downloading the same sort of data Mr. Lamb earlier identified as vulnerable and subject to manipulation. *See* Lamb Aff., ¶ 8. Also available on the CES site were training videos, one of which instructed election officials to download potentially corrupted files from the CES website (elections.kennesaw.edu) to a memory card and to then insert the infected memory card into their local vote

counting system. *See* Lamb Aff., ¶ 11. In this manner, malware could be spread throughout the system.

On March 1, 2017, Mr. Grayson notified KSU of the issue, and within days the servers were taken off line and removed from the facilities at KSU. Soon thereafter, the FBI took possession of the servers for analysis. Following that analysis, the servers were returned to the Secretary of State's office. As the Court noted in its September 17, 2018 Preliminary Injunction Order, "on July 7, 2017, four days after this lawsuit was originally filed...all data and hard drives of the University's 'elections.kennesaw.edu' server were destroyed.² 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 'elections.kennesaw.edu' server—was also destroyed." *See* Doc. 309, p. 9.³

² Federal Express delivered a copy of the Complaint in this action to the Secretary of State's office on July 6, 2017, the day before the first server was wiped and its data destroyed. *See* Federal Express receipt attached hereto as Exhibit "B."

³ The FBI took possession of the two servers soon after they were taken off line by CES and made a forensic image of one of the servers.

The destruction of the servers likewise destroyed any evidence that might have existed as to who gained unauthorized access to the servers.⁴ Additionally, the records on the server would have shown whether and to what extent malevolent actors removed or modified files or code that controlled the machines, or downloaded malware into the system that had the capacity to change votes and election outcomes.

For a period of at least six months prior to the destruction of the servers and, likely, much longer, critical election infrastructure impacting every county's election

⁴ “Foreign governments may engage in cyber operations targeting the election infrastructure and political organizations in Georgia and engage in influence operations that aim to interfere with the 2018 U.S. elections,” according to a memo by the U.S. Department of Homeland Security Southeast region addressing “a Georgia Perspective on Threats to the 2018 U.S. Elections.” The Oct. 2, 2018, memo warned Georgia that “cyber actors and foreign influencers ... may intend to disrupt political processes, sway public opinion, or to support or undermine certain political organizations.” https://www.law.com/dailyreportonline/2019/07/15/georgia-lawyers-argued-2018-voter-machines-were-safe-but-the-state-was-already-a-cyber-target/?cmp=share_twitter In July 2018, twelve Russian intelligence officers were indicted by the Justice Department. The indictment alleged that the accused had conspired to hack into computer systems involved in U.S. elections, which included “scoping out the websites of unidentified counties in ...Georgia to identify vulnerabilities they could use to access back-end servers.” See <https://www.politico.com/magazine/story/2018/07/18/mueller-indictments-georgia-voting-infrastructure-219018>

set up was easily accessible to any malicious actor who possessed even modest computer skills.

Ironically, when Plaintiffs, who are plainly committed to protecting the security of election systems in the State, have sought access to the GEMs database to discover the nature and scope of historical security breaches, Defendants have cynically purported to transform themselves into ardent advocates and vigilant protectors of election security. The transformation appears to have more to do with litigation strategy and political self-preservation than any authentic concern about election security.

The Demands for Preservation of Evidence

Since the destruction of the servers, Defendants have been warned and instructed multiple times to preserve all documents, records, and relevant evidence related to this matter. That follows is a description of ten (10) events that should have compelled Defendants to undertake immediate preservation efforts:

(1) The first action challenging the use of DREs in Georgia elections was filed on April 25, 2017.

(2) This action was filed on July 3, 2017, plainly triggering Defendants' duty to preserve relevant information, documents, and data.

(3) On July 10, 2017, Bryan Ward of Holcomb Ward, on behalf of Plaintiffs, sent an email message to the County Defendants demanding that all election materials from the June 20, 2017 election be preserved, including all storage media (i.e., memory cards) and demanding that all activities resulting in the destruction or modification of data cease.⁵

(4) Thereafter, evidence preservation was discussed during a September 5 and 6, 2017 meet and confer.

(5) The discussion of the meet and confer was memorialized and confirmed by a subsequent letter from Steptoe Johnson to Defendants on September 12, 2017.⁶

(6) The Coalition Plaintiffs' counsel also sent a preservation letter to Defendants on December 21, 2017, requesting the preservation of memory cards, resident DRE memories, files, databases, system logs, and flash drives used with the GEMs server and the Election Night Reporting server, and other evidence relevant to the subject matter of this action.⁷

⁵ See email from Mr. Ward attached hereto as Exhibit "C." _

⁶ See September 12, 2017 letter from Joe Robert Caldwell, Jr. (of Steptoe & Johnson) to all of Defendants' then-counsel, attached hereto as Exhibit "D."

⁷ The December 21, 2017 letter from William Brett Ney is attached hereto as Exhibit "E."

(7) Most importantly, on December 15, 2017, this Court entered an Order directing the parties to preserve “all evidence relevant to claims and defenses in this litigation...” The Court instructed that if there should be any dispute or confusion about compliance with the Order, the parties were to confer, and, if the issue could not be resolved, the parties should seek direction from the Court.

(8) On June 21, 2018, in anticipation of discovery eventually opening, Coalition Plaintiffs’ counsel Robert McGuire sent an email to Defendants Fulton County and Nonparties Cobb and Dekalb Counties, copying counsel for the State Defendants, advising them of their obligation to seek Plaintiffs’ consent before the “release of electronic records stored on DREs and their memory cards from [their] preservation obligations.”⁸

(9) Because discovery had been stayed in the action as of October 26, 2017, the State Defendants announced in a filing entitled, “State Defendants’ Notice of Intent to Serve Subpoena” (the “Notice of Intent”) their intention to serve a subpoena on the FBI for the purpose of “attempt[ing] to retain and secure the image [of the main KSU server made by the FBI] in the event it is later needed in this case for purposes of discovery.”⁹ Attorney Christina Correia of the Attorney General’s office

⁸ The June 21, 2018 email from Mr. McGuire is attached hereto as Exhibit “F.”

⁹ See Notice of Intent attached hereto as Exhibit “G.”

represented to the parties that it was the intention of the AG's office to store a copy of the image at the Secretary of State's office during the pendency of the litigation.¹⁰

(10) The Court's December 15, 2017 Order thereafter directed "the State Defendants...to communicate on a timely basis with all relevant third parties, such as the Federal Bureau of Investigation, regarding assistance in the immediate preservation of relevant data; data storage; media devices, discs and tapes; and other relevant software, data and hardware in this case." *See* Doc. 112, p. 2. Rather than follow that direction, the State Defendants did the exact opposite. The Notice of Intent suggests that the State Defendants knew that the FBI would, as a matter of standard operating procedure, dispose of the image after its investigation was complete, and the State Defendants' subsequent conduct indicates that is exactly what the State Defendants wanted to happen. After the "head feint" of filing the Notice of Intent, the State Defendants never filed or served the FBI with any subpoena nor did they make any other effort to "timely" secure the forensic image from the FBI, apparently hoping the FBI would destroy it.

The relevant elections for the purposes of this litigation included, but are not limited to, elections held in November 2016, April 2017, June 2017, November

¹⁰ *See* Ms. Correia's email of October 26, 2017, attached hereto as Exhibit "H."

2017, December 2017, May 2018, July 2018, November 2018, and December 2018 (the “Relevant Elections”). Cumulatively, in their demands for preservation of evidence made by Plaintiffs and the Court, Defendants were directed to preserve electronic information relevant to the conduct of elections dating back to November 2016. Defendants have, again, done the exact opposite—even after the Court made its concerns about spoliation plain.

The Spoliation: Memory Cards

When an elector votes on a DRE, her votes are recorded simultaneously on the machine’s internal memory and on the removable memory card, creating what should be an identical, but independent, record that could be compared if a memory card is defective or a discrepancy is noted. Data from each machine’s memory card is later downloaded into the county GEMS server to tabulate the votes. When the poll closes, the poll workers prompt the GEMS server to tally all downloaded votes. As was demonstrated in a live hearing before the Court, the DRE memory cards can be a conduit for delivering malware into the system. According to a Princeton University study, “An attacker who gets physical access to a machine or its

removable memory card for as little as one minute could install malicious code.”¹¹ A contaminated memory card can change the votes cast and can affect the outcome of elections. Accordingly, memory cards can be a critical piece of evidence in connection with uncovering whether an election’s outcome has been manipulated.¹²

In each election, some 30,000 to 40,000 memory cards are used. Since they sent the first preservation letter, Coalition Plaintiffs have demanded that Defendants preserve memory cards used in each of the Relevant Elections. Complying with such a request would be simple and easy. If the State Defendants did not have sufficient memory cards because some were sequestered for preservation purposes, the State Defendants could have purchased additional cards which are commercially available at minimal cost. They did not. If the State Defendants did not wish to buy new cards, they could have made forensic images of the used cards before using them again. They did not. If the State Defendants found either of those options unattractive, they could have approached Plaintiffs and sought some accommodation regarding preservation. They did not. Instead, the State Defendants ignored all of

¹¹ <https://whowhatwhy.org/2018/11/20/georgia-runoff-will-likely-contaminate-voting-machines-as-evidence/> (hereinafter “Georgia Runoff Contaminates Voting Machines”) attached hereto as Exhibit “I.”

¹² The Court’s September 17, 2018 Order succinctly and correctly recites the mechanics of the election process using DREs. *See* Doc. 309, pp. 4-6.

Plaintiffs' preservation demands, the Court's directions, and the laws' requirements regarding preservation of memory cards, and, instead, have reused memory cards from the Relevant Elections, overwriting and destroying the data stored on those cards that could be of critical importance in this matter. Defendants ignored Plaintiffs' demands, the Court's directions, and the law's requirements and recklessly did what they felt like doing.

The Spoliation: DRE Machines

The State's DRE Internal Memory Rule provides that "election results, ballot styles, ballot images, and other information for each election stored in the internal memory storage of each DRE unit shall be maintained for a minimum of one month following each election after which time the results may be erased provided that there are no election contests pending concerning such election."

The purpose of the Internal Memory Rule is to ensure that election officials have at least some retained election data that could be examined in the event of election tampering or system compromise or malfunction.¹³ The information necessary, but, candidly, likely insufficient, to conduct such a forensic analysis is all

¹³ See Declaration of Richard A. DeMillo, ¶16, attached hereto as Exhibit "J." Dr. DeMillo's qualifications and experience are recited in his August 20, 2018 Declaration. (Doc. 277 at 52).

electronic information related to the casting of votes: a copy of cast vote records, ballot images, audit logs, the DRE internal memory and memory cards.¹⁴ Thus, “[p]reserving the electronic data in the internal memory of the DRE requires that no new election data be written onto the hard drive of the DRE machines, no further use after the close of the election, including recounts, and that the DRE machines thus preserved be strictly physically secured and not deployed to polling places.”¹⁵

Defendants have a long tradition of ignoring that rule that dates back to 2002.¹⁶ Most recently, Defendants re-used DRE machines from the November 6, 2018 elections to conduct the December 4, 2018 run-off elections. In blatant violation of the Rule, two weeks after the November election was complete, counties began conducting “Logistics and Accuracy” testing on DREs and programing the machines and loading new ballot layouts into the machines.¹⁷ Assertions by the Secretary of State’s office that such re-programing of DREs can be conducted in compliance with the DRE Internal Memory Rule have been described by cyber-

¹⁴ *Id.* at ¶17.

¹⁵ *Id.* at ¶19.

¹⁶ *See* “Georgia Runoff Contaminates Voting Machines,” p. 7.

¹⁷ *Id.*

security experts as “utter nonsense.”¹⁸ The use of the November 2018 DREs in the December 2018 run-offs was not just a violation of the Secretary of State’s own rules for conducting elections; it destroyed evidence possibly critical to the case. It is worth noting that, independent of spoliation rules, election officials have the duty under Georgia law to retain documents and data related to elections conducted in the state for a period of two years. O.C.G.A. § 21-2-52 provides as follows:

All primary and election documents in the office of the Secretary of State shall be preserved therein for a period of at least 24 months and then the same may be destroyed unless otherwise provided by law.

Additionally, O.C.G.A. § 21-2-73, provides as follows:

All primary and election documents on file in the office of the election superintendent of each county, municipal governing authority, superintendent, registrar, committee of a political party or body, or other officer shall be preserved therein for a period of at least 24 months and then the same may be destroyed unless otherwise provided by law.

In violation of these statutory mandates, Defendants have willfully destroyed critical evidence in this case. The Secretary of State’s office, while the Secretary of State was seeking the Governor’s office, retrieved the servers from the FBI and promptly and brazenly destroyed it, placing it beyond the reach of Plaintiffs, the Court, and the People. A more crass, callous and contumacious disregard of the law is difficult to imagine. What’s worse is that it appears that all of this was done under

¹⁸ *Id.* at 7-8.

the supervision of, if not by, government lawyers, who are held to a higher standard than private lawyers.¹⁹

Prejudice

The servers destroyed by the State Defendants were the repository of records that go to the most critical issues in this case: logging records that would reflect unauthorized access of the election servers; deleted files or manipulated data; implanted malware that, as this Court has seen, can actually change an elector's vote and thereby actually change an election result. This type of evidence is not merely relevant and unique, it is fundamental, and it is forever gone. After abundant notice of their well-known duty to preserve evidence, the State Defendants did not simply neglect to disable some automated purge function in their IT systems. Rather, they intentionally and calculatingly destroyed evidence. Such conspicuously outrageous conduct can only raise the question: What were the State Defendants trying to hide? Surely, to engage in conduct so odious that any junior lawyer would know it would

¹⁹ “[A] government attorney must be held to higher standard than a private attorney. A government lawyer ‘in a civil action or administrative proceeding’ is held to a higher standard than a private lawyer, because ‘government lawyers have “the responsibility to seek justice,” and “should refrain from instituting or continuing litigation that is obviously unfair.”’ *Freeport–McMoRan Oil & Gas Co. v. F.E.R.C.*, 962 F.2d 45, 47 (D.C.Cir.1992) (quoting Model Code of Professional Responsibility EC 7–14 (1981)). *United States v. Witmer*, 835 F. Supp. 208, 214–15 (M.D. Pa. 1993), aff'd, 30 F.3d 1489 (3d Cir. 1994).

expose them to sanctions, the evidence so disposed of must have been damning in the extreme.

The parties are just now beginning the discovery process, and the most critical pieces of evidence that could establish vulnerability, unauthorized access of malign actors, and possible result-changing manipulation of the Georgia election system have been intentionally destroyed. While the actual probative value of spoliated evidence will always, by its nature, be of question, the inescapable inference here is that the evidence contained on the CES/KSU servers, and likely on certain DREs and memory cards, was of such a nature that the State Defendants made the decision it could never be seen, and they have made sure it never will be. The inferences that should be drawn from these events and the State Defendants' conduct speak volumes as to what has occurred here and the likelihood that Plaintiffs will succeed on the merits. Defendants' spoliation of evidence should minimally result in a presumption that the evidence destroyed by Defendants would tend to prove the merits of Plaintiffs' claims and should weigh heavily in the Court's assessment of whether to grant injunctive relief.

Respectfully submitted this 25th day of July 2019.

/s/ Cary Ichter

CARY ICHTER

Georgia Bar No. 382515

cichter@ichterdavis.com

ICHTER DAVIS LLC

3340 Peachtree Road NE,
Suite 1530

Atlanta, Georgia 30326

Tel.: 404.869.7600

Fax: 404.869.7610

/s/Bruce P. Brown

Bruce P. Brown

Georgia Bar No. 64460

BRUCE P. BROWN LAW LLC

1123 Zonolite Rd.

Suite 6

Atlanta, Georgia 30306

(404) 881-0700

/s/ Ezra D. Rosenberg

Ezra D. Rosenberg

John Powers

Co-Director, Voting Rights Project

Lawyers' Committee for Civil Rights Under Law

1500 K Street, NW, Suite 900

Washington, DC 20005

(202) 662-8345 (office)

*Attorneys for Coalition for Good
Governance*

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRIAN KEMP, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing document has been prepared in accordance with the font type and margin requirements of LR 5.1, using font type of Times New Roman and a point size of 14.

/s/ Cary Ichter

Cary Ichter

EXHIBIT A

**IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA**

DONNA CURLING, an individual, et al.)	
)	
Plaintiffs,)	
)	
v.)	CIVIL ACTION
)	FILE NO.:
BRIAN P. KEMP, in his individual capacity)	
and his official capacity as Secretary of)	
State of Georgia and Chair of the)	
STATE ELECTION BOARD, et al.,)	
)	
Defendants.)	

AFFIDAVIT OF LOGAN LAMB

County of Fulton)
) ss.
 State of Georgia)

LOGAN LAMB ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am a cybersecurity researcher based in Atlanta. I have a BS and MS in computer engineering from University of Tennessee, Knoxville. I have worked professionally in cybersecurity since 2010. I started at Oak Ridge National Lab in the Cyber and Information Security Research group. At CISR I specialized in static and symbolic analysis of binaries. I also worked with embedded systems security and conducting security assessments for the federal government. I left ORNL in 2014 and joined Bastille Networks, a local startup where I am still employed. At Bastille Networks I specialize in wireless security and applications of software defined radio.

2. On August 23, 2016 I went to 130 Peachtree Street in an attempt to meet the Fulton County election supervisor Richard Barron with the hope of gaining access to voting systems equipment so that I could conducting a wireless security

assessment as a research project. There I was told to contact Merle King at Kennesaw State University because all election equipment is managed by the Center for Election Systems at KSU.

3. On August 24, 2016 I intended to contact Merle King. Prior to doing so, I wanted to check the Center for Election Systems public website to see if there were any public documents that could give me background on CES and Merle King. I used the search "site:elections.kennesaw.edu inurl:pdf" at www.google.com and discovered what appeared to be files relating to voter registration cached by google.
4. After this discovery, I wrote a quick script to download what public files were available here: <https://elections.kennesaw.edu/sites/> , at the time a publicly accessible site. After running the script to completion I had acquired multiple gigabytes of data. This data was comprised of many different files and formats, but among them were:
 - voter registration databases filled with personally identifiable information of voters (filename *PollData.db3*)
 - Election Management System GEMs databases (.gbf and .mdb extensions)
 - PDFs of election day supervisor passwords, for example:
 - *July 2016 Primary and NP Election Runoff Password Memo.pdf*
 - Windows executables and DLLs, for example:
 - *System.Data.SQLite.DLL*
 - *ExpDbCreate.exe*
 - *ExpReport.exe*
5. Besides leaking information, the server at elections.kennesaw.edu was running a version of Drupal vulnerable to an exploit called drupageddon. Using drupageddon, an attacker can fully compromise a vulnerable server with ease. A

public advisory for drupageddon was release in 2014, alerting users that attackers would be able to execute, create, modify, and delete anything on the server.

On August 28, 2016 I sent an email to Merle King notifying him of the vulnerabilities I found.

Hello Merle,

My name is Logan Lamb, and I'm a cybersecurity researcher who is a member of Bastille Threat Research Team. We work to secure devices against new and existing wireless threats: <https://www.bastille.net/>. This past Tuesday I went to Fulton County Government Center to speak with Rick Barron about securing voting machines against wireless threats. I was then directed to contact you and the center. I'd like to collaborate with you on securing our state's election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to contacting you, I discovered serious vulnerabilities affecting elections.kennesaw.edu.

The following google searches reveal documents that shouldn't be indexed and appear to be critical to the elections process. In addition, the Drupal install needs to be immediately upgraded from the current version, 7.31:

"site:elections.kennesaw.edu inurl:pdf"

I generally use this type of search to find documents on websites that lack search functionality. This search revealed a completely open Drupal install. Assume any document that requires authorization has already been downloaded without authorization.

"site:elections.kennesaw.edu L&A"

The second search result appears to be for disseminating critical voting system software. This is especially concerning because, as the following article states, there's a strong probability that your site is already compromised.
<https://www.drupal.org/project/drupalgeddon>
<https://www.drupal.org/SA-CORE-2014-005>

If you have any questions or concerns please contact me. I'm able to come to the center this Monday for a more thorough discussion.

Take care,
Logan

6. After having a brief conversation with Mr. King on August 29, 2016 and being assured that the issues would be remediated, I dropped the issue.

7. In late February, 2017 I told my colleague Chris Grayson about what transpired in August. He quickly confirmed the leaking of information had not been appropriately remediated. I tweaked my script and checked to see if it worked as it had in August.
8. The script was able to download the publicly available information. The data downloaded included the same data from the previous collection and new information relating to recent elections including:
 - More recent GEMs database files
 - Files relating to the presidential election, e.g.
 - *November 2016 General Election Day Password Memo.pdf*
 - *November 2016 General Voter Lookup Password Memo.pdf*
 - Very recent files, e.g. *064 (1-10-2017).pdf*
9. Given the severity and ease with which an attacker can use drupageddon, an attacker would have easily been able to gain full control of the server at elections.kennesaw.edu had they so wanted.
10. Having gained control of the server, an attacker could modify files that are downloaded by the end users of the website, potentially spreading malware to everyone who downloaded files from the website.
11. In addition to the previously mentioned files on the server, there were multiple training videos. One of these training videos instructed users to first download files from the elections.kennesaw.edu website, put those files on a memory card, and insert that card into their local county voting systems.
12. Further Affiant sayeth not.


Logan Lamb

Sworn before me this 30 day of June, 2017, in June.


NOTARY PUBLIC



EXHIBIT B

Monday, October 23, 2017 at 2:50:44 PM Eastern Daylight Time

Subject: Fwd: FedEx Shipment 779560905340 Delivered**Date:** Thursday, July 6, 2017 at 12:04:33 PM Eastern Daylight Time**From:** Scott Holcomb**To:** Bryan Ward, Matt Hickman, Marvin Lim, Mr Aaron Wright, Marilyn Marks, Donna Price Studio, Donna Curling

FYI—delivered to the State Election Board (Brian Kemp, as Chair), in accordance with the statute.

Scott Holcomb**Holcomb + Ward, LLP****HW HOLCOMB
+ WARD LLP**

3399 Peachtree Road NE, Suite 400

Atlanta, Georgia 30326

404-601-2803 (Main)

404-387-0373 (Direct)

404-393-1554 (Fax)

scott@holcombward.comwww.holcombward.com

----- Forwarded message -----

From: <TrackingUpdates@fedex.com>**Date:** Thu, Jul 6, 2017 at 11:35 AM**Subject:** FedEx Shipment 779560905340 Delivered**To:** scott@holcombward.com

Your package has been delivered

Tracking # 779560905340


Ship date:
Wed, 7/5/2017**Bryan M. Ward**
Holcomb + Ward, LLP
ATLANTA, GA 30326
US**Delivery date:**
Thu, 7/6/2017 11:30 ar**Secretary Kemp, Chairman**
State Election Board
214 STATE CAPITOL SW
ATLANTA, GA 30334
US**FedEx®**

Shipment Facts

Our records indicate that the following package has been delivered.

Tracking number: 779560905340**Status:** Delivered: 07/06/2017 11:30
AM Signed for By: L.OFLER**Signed for by:** L.OFLER**Delivery location:** ATLANTA, GA

Delivered to:	Receptionist/Front Desk
Service type:	FedEx Standard Overnight
Packaging type:	FedEx Box
Number of pieces:	1
Weight:	2.00 lb.
Special handling/Services:	Deliver Weekday
Standard transit:	7/6/2017 by 3:00 pm

 Please do not respond to this message. This email was sent from an unattended mailbox. This report was generated at approximately 10:35 AM CDT on 07/06/2017.

All weights are estimated.

To track the latest status of your shipment, click on the tracking number above.

Standard transit is the date and time the package is scheduled to be delivered by, based on the selected service, destination, ship date. Limitations and exceptions may apply. Please see the FedEx Service Guide for terms and conditions of service, including the FedEx Money-Back Guarantee, or contact your FedEx Customer Support representative.

© 2017 Federal Express Corporation. The content of this message is protected by copyright and trademark laws under U.S. and international law. Review our [privacy policy](#). All rights reserved.

Thank you for your business.

EXHIBIT C

White, Tyechia

From: Bryan Ward <bryan.ward@holcombward.com>
Sent: Monday, July 10, 2017 5:32 PM
To: ACowart@law.ga.gov; RWillard@law.ga.gov; JColangelo@law.ga.gov;
CCorreia@law.ga.gov; JHeidt@law.ga.gov; ovbrantley@dekalbcountyga.gov;
LKJohnson@DeKalbCountyGa.gov; TGPhilli@DeKalbCountyGa.gov;
BDBryan@DeKalbCountyGa.gov; Patrise.Hooker@FultonCountyGa.gov;
Kaye.Burwell@FultonCountyGa.gov; Cheryl.Ringer@FultonCountyGa.gov;
David.Lowman@FultonCountyGa.gov; DWhite@hlclaw.com; SHegener@hlclaw.com
Cc: Marvin Lim
Subject: Curling et al. v. Kemp et al.; No. 2017CV292233
Attachments: CURLING v KEMP (2) - COMPLAINT WITH VERIFICATION AND EXHIBITS.PDF

Counsel,

I am counsel for the plaintiffs in the above-referenced matter, *Curling et al. v. Kemp et al.*; No. 2017CV292233 (the "Action") (Complaint attached). I am writing you as either the attorney listed online for one of the defendant entities in the above-referenced matter or as an attorney for a defendant entity in the now-dismissed *Curling et al. v. Kemp et al.*, No. 2017CV290630. The purpose of this email is to notify your clients of their obligation to take reasonable steps to preserve and retain all hard copies and electronically stored information, as defined by Rule 34 of the Federal Rules of Civil Procedure, and all other documents and physical evidence relevant to this Action. To fulfill your preservation obligation, you must take reasonable steps to preserve all hard copy documents, physical evidence, and electronically stored information relevant to this Action, including, but not limited to

- suspending the Defendant entities' data destruction and backup tape recycling policies;
- preserving relevant software, including legacy software (unless an exact copy or mirror image is made and stored) and hardware that is no longer in service but was in service during the relevant time period;
- retaining and preserving necessary information to access, review and reconstruct (if necessary) relevant electronic data, including identification codes and passwords, decryption applications, decompression software, reconstruction software, network access codes, manuals and user instructions;
- retaining and preserving all backup tapes or other storage media; and
- any other reasonable steps necessary to prevent the destruction, loss, override or modification of relevant data either intentionally or inadvertently, such as through implementation of a pre-existing document retention policy.

This preservation obligation includes all election materials for the June 20 election, including, in particular, **memory cards** (PCMCIA cards) used in that election. In addition, we are available to confer about the retention and security of the voting machines and GEMS server used in the June 20 and April 18 elections. Until such time, those machines should not be disturbed, tested, or changed in any way.

The foregoing list is not exhaustive, and you and your clients must preserve all documents, physical evidence, and information relevant to this Action.

Your clients' failure to preserve relevant data may constitute spoliation of evidence, which may subject your and/or your clients to sanctions. We trust that you and your clients will preserve for the duration of this Action all relevant hard copy documents, physical items, and electronically stored information. In the event of a dispute arising out of your failure to preserve documents, we will rely on this email in court as evidence of our request and additional notice of your and your clients' preservation obligations.

We look forward to working with you in this matter. Please contact me if you have any questions.

Bryan M. Ward



3399 Peachtree Road NE, Suite 400

Atlanta, Georgia 30326

404-892-5695 (Direct)

404-601-2803 (Main)

404-393-1554 (Fax)

bryan.ward@holcombward.com

www.holcombward.com

EXHIBIT D

Joe Robert Caldwell, Jr.
202 429 6455
jcaldwell@step toe.com
1330 Connecticut Avenue, NW
Washington, DC 20036-1795
202 429 3000 main
www.step toe.com



September 12, 2017

BY ELECTRONIC AND REGULAR MAIL

Cristina Correia
Josiah Benjamin Heidt
Elizabeth Ahern Monyak
Attorney General's Office-Atl
Department of Law
40 Capitol Square, SW
Atlanta, GA 30334
404-656-7063

Cheryl Ringer
David R. Lowman
Kaye Woodard Burwell
Office of Fulton County Attorney
Fulton County Government Center
141 Pryor Street, S.W.
Suite 4038
Atlanta, GA 30303
404-612-0263
Email: cheryl.ringer@fultoncountyga.gov

Bennett Davis Bryan
DeKalb County District Attorney's Office
Stone Mountain Judicial Circuit
556 North McDonough Street
Suite 700
Decatur, GA 30030
404-687-3815
Email: bdbryan@dekalbcountyga.gov

Daniel Walter White
Haynie Litchfield Crane & White
222 Washington Avenue
Marietta, GA 30060
770-422-8900
Fax: 770-424-8900
Email: dwhite@hlclaw.com



Re: *Donna Curling, et al. v. Brian P. Kemp, et al.*, Civil No. 17-cv-02989-AT, United States District Court for the Northern District of Georgia

Dear Counsel;

As counsel for Plaintiffs in this action, and following up on our “meet and confer” conference calls on September 5 and 6, 2017, this letter is written to request that Defendants take reasonable steps to preserve all documents and records, including but not limited to all electronically stored information (“ESI”), that are relevant to the allegations in the pleadings in this action, or that are reasonably likely to lead to the discovery of admissible evidence.

Please ensure that Defendants preserve not merely the DRE voting machines, but all equipment, hard copy documents, and electronic data/information related to the November 2016, April and June 2017 elections including but not limited to:

1. DREs (Accuvote TS machines);¹
2. 2 Optical Scanners;
3. TSx machines (whether used in voting or electronic transmission of voting data);
4. voter registration records;
5. poll books and all related electronic and paper data;
6. 10 voter access cards to be selected by the Plaintiffs from a list of inventory supplied by the Defendants;
7. communications related to the allegations in the Complaint (including, but not limited to, requests to recanvas, concerns about the voting system, certification of the voting system, and internal, non-privileged communications regarding the same), including the planning for the November 2016 general election;
8. internal or external investigations related to the November 2016, April 2017 and June 2017 elections (including, but not limited to, any software issues creating problems with voter registration, voter records, or voters ability to vote, or location for voting, and any forensic review or investigation);
9. card creators;

¹ As Defendants are aware, Plaintiffs remain amenable to releasing voting machines needed for the November 2017 election after being supplied with an inventory of machines and other equipment needed for their consideration.



10. GEMS databases;
11. election night reporting records and data (including the Election Night Reporting server activity logs);
12. memory cards for all equipment;
13. Election Media Processors;
14. modem transmission network logs;
15. any external storage device, servers, component, or other technology used to create, program, read, store, or transfer any of the above.

With respect to electronic records, we expect that Defendants have already imposed a litigation hold to preserve and retain all potentially pertinent ESI within their possession, custody or control, consistent with their obligations under the Federal Rules of Civil Procedure. For purposes of this notice, ESI shall include, without limitation, all electronic mail ("email") files and attachments, backup email files (including backup media, such as Microsoft Exchange server backup tapes), text files (including word processing documents), data files, program files, spreadsheets, graphical image files (including .JPG, .GIF, .BMP, .TIFF and .PDF files), databases, voicemail messages and files, calendar and scheduling information, computer system activity logs (including network, web, and server logs), external storage devices, servers, or other technology used to create, program, read, store, or transfer data, and backup tapes. It shall also include all file fragments, residual and hidden data, deleted files and other electronically recorded information to the extent that the preservation of such data is reasonably calculated to lead to the retrieval of any relevant deleted information.

The duty of good faith which arises from the Federal Rules of Civil Procedure relating to the discovery of electronically stored information requires Defendants to take all steps necessary to prevent the loss of any relevant information, even if it is believed not to be reasonably accessible. Please also note that electronically stored information typically contains relevant, discoverable information beyond what is apparent to the viewers, *e.g.*, embedded data or metadata. As a result, Defendants must preserve all electronically stored information in its original electronic form, even where paper copies might exist. Because electronically stored information can be easily modified, deleted or otherwise corrupted, Defendants must take all necessary steps to make sure that all electronically discoverable data is preserved. This obligation includes the requirement that Defendants confirm that data is not altered or otherwise destroyed from automatic functions occurring during the routine operation of any electronic information systems, upgrades or the recycling of computer-related hardware or software. This preservation requirement includes, but is not limited to, the obligation to suspend any such operations, upgrades, or recycling features or protocols (including any document or data destruction policies) pending resolution of potential claims against Defendants.

We reserve the right to supplement this demand as investigation and discovery proceed. Of course, if you have any questions regarding any of the foregoing, please contact me directly.

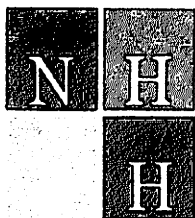


Sincerely,

A handwritten signature in black ink, appearing to read "Joe Caldwell".

Joe Robert Caldwell, Jr.

EXHIBIT E



NEY HOFFECKER PEACOCK & HAYLE, LLC
ATTORNEYS AT LAW

ONE MIDTOWN PLAZA, SUITE 1010
1360 PEACHTREE STREET NE
ATLANTA, GEORGIA 30309

WILLIAM BRENT NEY

Direct Dial 404-842-7232
Fax 470-225-6646
william@nhphlaw.com
www.nhphlaw.com

December 21, 2017

Cheryl Ringer
Office of Fulton County Attorney
Fulton County Government Center
141 Pryor Street, S.W. Suite 4038
Atlanta, GA 30303

**BY U.S. MAIL
AND EMAIL**

Re: *Curling et al. v. Kemp et al.*, United States District Court for the Northern District
of Georgia, State of Georgia, Civil Action File No. 1:17-cv-2989-AT

Ms. Ringer:

My firm represents Coalition for Good Governance in the above referenced matter. I am writing to alert you of the need to preserve documents and data for potential discovery requests that we anticipate filing with Fulton County when the discovery stay is lifted. The following request is for preservation of information related to the November 7, 2017 and December 5, 2017 elections, runoffs and recounts conducted by Fulton County Board of Elections. Please communicate with your clients that the documents and data listed below should be preserved in anticipation of our discovery requests:

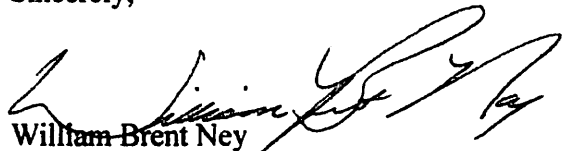
1. All DRE, Optical Scan and Express Pollbook memory cards created for use.
2. Resident memory data on DRE's used in the specified elections.
3. All programming files, databases and system logs for the GEMS server and Election Night Reporting server.
4. Flashdrives or other media used to transfer data between the GEMS server and the Election Night Reporting server.
5. Maintenance records, repair records, error reports relating to any and all voting system components.
6. All ballots, balloting materials, chain of custody records and communications related to election processing for the specified elections.
7. All system logs and transmission data records related to transmission of data via TSx machines in the specified elections.

Cheryl Ringer
Office of Fulton County Attorney
December 21, 2017
Page 2

The above list does not supersede the litigation hold requests previously transmitted in this matter, but supplements those requests, and your clients' ongoing obligations to comply with Georgia's election code preservation statutes. In the event that the DREs or memory cards are required for use in upcoming elections prior to the initiation of discovery, I am sure that we can create a workable arrangement for mutually satisfactory sampling or imaging of the data we will require in discovery.

If you have any questions regarding this matter, please contact my office.

Sincerely,



William Brent Ney
Attorney for Coalition for Good Governance

WBN/bn

C:	Marilyn Marks	By Email
	Robert McGuire	By Email
	John Frank Salter, Jr.	By Email
	Roy E. Barnes	By Email
	Robert S. Highsmith	By Email
	Edward Bruce Schwartz	By Email
	Joe Robert Caldwell, Jr.	By Email
	Bryan Ward	By Email
	Aaron Wright	By Email

EXHIBIT F

From: Rob McGuire <ram@lawram.com>

Date: Thursday, June 21, 2018 at 2:43 PM

To: Daniel Walter White <dwhite@hlclaw.com>, Bennett Davis Bryan

<bdbryan@dekalbcountyga.gov>, "Laura K. Johnson" <ljohnson@dekalbcountyga.gov>, Cheryl Ringer <Cheryl.ringer@fultoncountyga.gov>, David Lowman

<david.lowman@fultoncountyga.gov>, Kaye Burwell <Kaye.burwell@fultoncountyga.gov>

Cc: John Salter <john@barneslawgroup.com>, Roy Barnes <Roy@barneslawgroup.com>, "Adam M. Sparks" <sparks@khlawfirm.com>, "Chapple, Catherine L." <CChapple@mofo.com>,

Conaway <jconaway@mofo.com>, "David D. Cross" <DCross@mofo.com>, "Halsey G. Knapp, Jr." <hknapp@khlawfirm.com>, "Jane P. Bentrrott" <JBentrrott@mofo.com>, John Carlin

<jcarlin@mofo.com>, Miriyala <amiriyala@mofo.com>, Robert Manoso

<rmanoso@mofo.com>, Bruce Brown <bbrown@brucepbrownlaw.com>, Cary Ichter

<Clichter@IchterDavis.com>, "william@nhphlaw.com" <william@nhphlaw.com>, Marilyn Marks <marilyn@aspenoffice.com>

Subject: Categories of DREs to Identify and Preserve pending Release of Any from Litigation Hold

Counsel for Defendant Fulton County and for nonparties Cobb County and DeKalb County,

On behalf of the Coalition Plaintiffs I am writing to give you notice—which you already have from my previous correspondence—that we have not yet received the information that we require in order to consent to the release of electronic records stored on DREs and their memory cards from your preservation obligations. In order to be able to go through the exercise of identifying which DREs are of less interest to us (and which we can thus consent for you to remove from litigation hold), we have to receive the information we have previously requested. Please inform us as to when you plan to supply the vote tally information and complete the recap sheet information, giving us reasonable time to respond in order for you to prepare machines for the upcoming July 24 election.

Also, because discovery has not begun and we cannot research the records ourselves to locate the specific electronic records we seek to review, I am writing to provide the counties with 15 specific criteria we plan to use to make discovery requests. This way the counties themselves can do the identifying and can ensure that the DREs matching our criteria continue to be preserved. All of the DREs that fall into any of the 15 categories listed in the attachment to his email will contain electronic records that we intend to request in discovery, as soon as the current stay is lifted by the Court. Accordingly, none of the DREs in any of these 15 these categories can be released from the litigation hold. As more information becomes

available we will expand this list to include other criteria before the release date to be agreed on.

With this list, all three counties now have advance notice that they need before the original deadline of tomorrow to identify, sequester, and continue to preserve all the electronic records on all of the DREs in these 15 categories—and none of the DREs in any of these 15 categories can be released from the litigation hold. To restate the point in other words, you have a duty not to destroy evidence on the DREs in these 15 categories because you are on clear notice that we intend to seek electronic records from the DREs that meet these 15 criteria as soon as discovery opens. You will be at risk of engaging in spoliation and contempt of court if you destroy evidence on any of the DRE machines that are included in any of the 15 categories we have identified in the attached list.

We also wish to conduct discovery on DREs that we will select based on their recorded vote counts by contest. You have not provided us this information as we have requested, and we are still expecting it to be delivered prior to our consenting to the release of any DREs or other electronic records from the current litigation hold. -By providing you the attached list of categories, we are not waiving our objection to releasing any DRE electronic records from the litigation hold prior to receiving the information we have requested on this list and the in our previous request for vote tallies and machine use by serial number. When you do provide the information we previously requested concerning vote counts and concerning your inventory of machines, then we will be able to submit a more detailed list of DREs for you to preserve, and we may be able to identify machines that can be released from litigation hold with our consent at that time.

Note that the attached list only covers electronic records on the DREs that are in these 15 categories and their memory cards. All memory cards from all other DREs used in any of the Relevant Elections (even DREs that are not in the 15 categories) must continue to be preserved under both the Court's Order (Doc 122) and Plaintiffs' prior litigation hold letters. This preservation requirement exists pursuant to the 22-month federal statutory federal requirements and pursuant to Diebold's Security Policies as published in GEMS 1.18 Election Administrator's Guide. By providing categories of DREs that are of interest of the attached list, we do not suggest that the memory cards from all other DREs do not need to be preserved—they must be.

Please see Exhibit 1 attached to this email.

Best,

Robert McGuire

ROBERT A. MCGUIRE, III

***** NOTE NEW CONTACT DETAILS BELOW *****

SHAREHOLDER | THE ROBERT MCGUIRE LAW FIRM

1624 MARKET ST STE 226 #86685, DENVER, CO 80202-2523 | 113 CHERRY ST #86685, SEATTLE, WA 98104-2205

E: ram@lawram.com | T/F: 720.420.1395 | T/F: 253.267.8530 | www.lawram.com

This communication is confidential, may be privileged and is meant only for the intended recipient. If you are not the intended recipient, please notify the sender by reply and delete the message from your system. Any unauthorized dissemination, distribution or copying hereof is prohibited.

Exhibit 1: List of Criteria for DRE Electronic Record Preservation

Date: June 21, 2018

Exhibit 1 Advance Preliminary List of Criteria for DRE Electronic Record Preservation

This list will be supplemented by additional list of specific machines and other categories of machines for which the electronic records must be preserved. While this list focuses primarily on the electronic records in the internal memories of the DREs it should be understood that all memory cards associated with the DREs and other electronic equipment must be preserved as well. Unless otherwise specified the request relates to all DREs used in all relevant elections including November 2016, April 2017, June 2017, November 2017, December 2017 and May 2018.

1. All DREs in which blank ballots were recorded. (Voter cast ballot with no selections.)
2. All DREs which were put in service in polling place and no ballots were cast on them.
3. All DREs which were prepared as backups but not put in service.
4. (Fulton only) All (TSx) DREs used for electronic election night transmission of results to the GEMS server.
5. All DREs from polling places in which the difference is greater than 3 between voter applications and ballots cast.
6. All DREs taken out of service during any relevant election because of voter complaints.
7. All DREs reported as “frozen” during voting day.
8. All DREs recording votes from precincts recording over 90% turnout according to the Clarity election night reporting statistics on the Secretary of States’ website.
9. All DREs recording votes from precincts recording less than 35% turnout in the November 2016 election according to the Clarity election night reporting statistics on the Secretary of States’ website.
10. All DREs that issued incorrect ballots to voters, (whether or not the voter reported the wrong ballot issuance.)
11. All DREs used as precinct accumulator machines.
12. All DREs used in polling places in which fewer memory cards were uploaded than the number of machines in the polling place.
13. All DREs and memory cards for which efforts were made to “wipe” or delete electronic election data from the internal memory from any of the relevant elections, as discussed on the parties’ joint phone call on May 4, 2018.

Exhibit 1: List of Criteria for DRE Electronic Record Preservation

Date: June 21, 2018

14. (Fulton County) All DREs used to record votes in the November 2016 election for precinct 02J.
15. (Fulton County) All DREs used to record a vote in CD6 from precinct 02J in the November 2016 election.

EXHIBIT G

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, et al.,)	
)	
Plaintiffs,)	CA No. 1:17cv02989-AT
)	
v.)	
)	
BRIAN KEMP, et al.,)	
)	
<u>Defendants.</u>)	

STATE DEFENDANTS' NOTICE OF INTENT TO SERVE SUBPOENA

Pursuant to Rule 45(a)(4) of the Federal Rules of Civil Procedure, the State Defendants hereby notify all parties that they intend to serve a subpoena on the Atlanta Division of the Federal Bureau of Investigation ("FBI") to obtain a copy of the forensic image that was made by the FBI of the Kennesaw State University Center for Election Systems ("CES"s) server in March of 2017. *See* Exhibit 1 attached hereto.

Discovery in this case is stayed pursuant to the Court's September 5, 2017 (Doc. 56), and the State Defendants are not engaging in any discovery with respect to this drive and will not access it unless and until the stay of discovery is lifted (in the event that the State Defendants' Motion to Dismiss is not granted or only partially granted). This subpoena is being issued at this time in an attempt to retain and secure the image in the event it is later needed in this case for purposes of

discovery. The Court's Order staying discovery encourages the parties to take steps during the stay to facilitate an orderly and prompt resolution of the case. (Doc. 56).

The original CES server was wiped on July 7, 2017, prior to service of this lawsuit on any Defendant in this case; however, given that the FBI took a forensic image of the server during the 2-week period in March of 2017 when the server was in the FBI's possession, it is possible to obtain a copy of the image of that server as it appeared in March of 2017 when it was in FBI custody. Given that the FBI has closed its investigation of this matter, the FBI's forensic image was scheduled for destruction under standard FBI record retention policies and has been or soon will be wiped. Prior to the scheduled wiping of the original forensic image, the FBI made a copy of that image, which will be installed on a blank drive to be provided by the Georgia Secretary of State's Office to the FBI. This subpoena will seek production of that copy of the forensic image of the server taken by the FBI in March of 2017.

Upon taking possession of the drive with the forensic image copied on to it, the drive will be secured and taken by representatives at the Secretary of State's office to a secured storage facility at their Office. It will not be accessed by the State Defendants (or their counsel) unless and until discovery begins in this case.


The State Defendants emphasize that by taking these actions, they are not acknowledging that the server taken by the FBI has any relevance to the Plaintiffs' claims in this lawsuit regarding the reliability of DREs or the electronic voting system in Georgia. The image is being obtained and preserved in an abundance of caution in the event that discovery of the forensic image is later determined to be relevant and discoverable.

Respectfully submitted,

CHRISTOPHER M. CARR
Attorney General 112505

ANNETTE M. COWART 191199
Deputy Attorney General

RUSSELL D. WILLARD 760280
Senior Assistant Attorney General


CRISTINA M. CORREIA 188620
Assistant Attorney General

ELIZABETH A. MONYAK 005745
Assistant Attorney General

JOSIAH B. HEIDT 104183
Assistant Attorney General

Georgia Department of Law
40 Capitol Square SW
Atlanta, GA 30334
404-656-7063

Attorneys for State Defendants

Please address all
Communication to:
CRISTINA CORREIA
Assistant Attorney General
40 Capitol Square SW
Atlanta, GA 30334
ccorreia@law.ga.gov
404-656-7063
404-651-9325

CERTIFICATE OF SERVICE

I hereby certify that on this date I have e-mailed and mailed by U.S. mail,
U.S. postage prepaid, a copy of the foregoing Notice, addressed to the following:

Bryan Ward
Marvin Lim
Holcomb + Ward LLP
3399 Peachtree Rd NE, Suite 400
Atlanta, GA 30326
Bryan.Ward@holcombward.com
Marvin@holcombward.com

Joe Caldwell, Jr.
Edward Schwartz
Steptoe & Johnson-DC
1330 Connecticut Avenue, N.W.
Washington, DC 20036-1795

Overtis Hicks Brantley
Bennett D. Bryan
DeKalb County Law Department
1300 Commerce Drive 5th Floor
Decatur, GA 30030

Patrise M. Perkins-Hooker
Kaye Burwell
Cheryl Ringer
Fulton County Attorney's Office
141 Pryor Street SW Suite 4038
Atlanta, GA 30303
Facsimile: (404) 730-6324

Daniel W. White
Haynie, Litchfield, Crane & White, PC
222 Washington Avenue
Marietta, Georgia 30060

This 26th day of October, 2017.

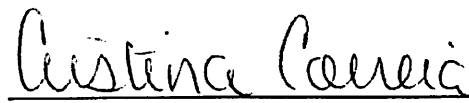

Assistant Attorney General

EXHIBIT 1

U.S. District Court (Rev. 02/14) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of Georgia

Donna Curling, et al.

Plaintiff

v.

Brian Kemp, et al.

Defendant

Civil Action No. 1:17-cv-2989-AT

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Kristy Green
Chief Division Counsel, FBI, Atlanta Office
(Name of person to whom this subpoena is directed)

☒ **Production:** YOU ARE COMMANDED to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: copy of forensic image that was made by the FBI of the Center for Elections Systems' election server in March of 2017 following FBI taking possession of that server (a Dell Power Edge R610 with DNS name elections.kennesaw.edu)

Place: FBI, Atlanta Division 3000 Flowers Road South Atlanta, Georgia 30341	Date and Time: <i>Mutually agreeable time and place</i>
---	--

☐ **Inspection of Premises:** YOU ARE COMMANDED to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:
--------	----------------

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 10/23/2017

CLERK OF COURT

OR

Elizabeth A. Monyak
Elizabeth A. Monyak
Attorney's signature

Signature of Clerk or Deputy Clerk

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Brian Kemp, Center for Elections Systems, Merle King, CES, SEB, and SEB members, who issues or requests this subpoena, are: Elizabeth A. Monyak, 40 Capitol Square, SW, Atlanta, Georgia 30334; emonyak@law.ga.gov; 404-463-3630

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

AO 88B (Rev. 02/14) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action (Page 2)

Civil Action No. 1:17-cv-2989-AT

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____
on *(date)* _____.

☐ I served the subpoena by delivering a copy to the named person as follows: _____

_____ on *(date)* _____; or

☐ I returned the subpoena unexecuted because: _____
_____.

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also
tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of
\$ _____.

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ 0.00.

I declare under penalty of perjury that this information is true.

Date: _____
_____ *Server's signature*

Printed name and title

Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)**(c) Place of Compliance.**

(1) For a Trial, Hearing, or Deposition. A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

- (A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or
- (B) within the state where the person resides, is employed, or regularly transacts business in person, if the person
 - (i) is a party or a party's officer; or
 - (ii) is commanded to attend a trial and would not incur substantial expense.

(2) For Other Discovery. A subpoena may command:

- (A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and
- (B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) Avoiding Undue Burden or Expense; Sanctions. A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) Command to Produce Materials or Permit Inspection.

(A) Appearance Not Required. A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) Objections. A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

- (i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.
- (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) Quashing or Modifying a Subpoena.

(A) When Required. On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

- (i) fails to allow a reasonable time to comply;
- (ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);
- (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or
- (iv) subjects a person to undue burden.

(B) When Permitted. To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

- (i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) Specifying Conditions as an Alternative. In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

- (i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and
- (ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) Producing Documents or Electronically Stored Information. These procedures apply to producing documents or electronically stored information:

(A) Documents. A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) Form for Producing Electronically Stored Information Not Specified. If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) Electronically Stored Information Produced in Only One Form. The person responding need not produce the same electronically stored information in more than one form.

(D) Inaccessible Electronically Stored Information. The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) Claiming Privilege or Protection.

(A) Information Withheld. A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

- (i) expressly make the claim; and
- (ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) Information Produced. If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT H

From: Cristina Correia [mailto:ccorreia@law.ga.gov]
Sent: Thursday, October 26, 2017 2:00 PM
To: 'Caldwell, Joe' <jcaldwell@Steptoe.com>
Cc: 'Ringer, Cheryl' <Cheryl.Ringer@fultoncountyga.gov>; 'Bryan, Bennett D (benbryan@dekalbcountyga.gov)' <benbryan@dekalbcountyga.gov>; 'Burwell, Kaye' <Kaye.Burwell@fultoncountyga.gov>; Elizabeth A. Monyak <emonyak@law.ga.gov>; 'Daniel White (dwhite@hlclaw.com)' <dwhite@hlclaw.com>; 'Bryan Ward' <bryan.ward@holcombward.com>; 'Schwartz, Edward' <eschwartz@steptoe.com>; Josiah Heidt <JHeidt@LAW.GA.GOV>; 'Jeff Milsteen' <jmilstee@kennesaw.edu>
Subject: RE: Curling v. Kemp: Clarification of Litigation Hold regarding CES and Kennesaw State

Joe,

We have learned from the FBI that they do have a copy of the forensic image that they took of the CES server which they seized last March. Please see the attached Notice of Intent to Serve a Subpoena, which explains that we are seeking a copy of the forensic image from the FBI and that we intend to store that copy in a secure location at the Office of the Secretary of State during the pendency of this litigation.

As always, please feel free to contact me should you have any questions.

Best,
Cris

EXHIBIT I

From: Transparent Elections <georgiapaperballots@gmail.com>

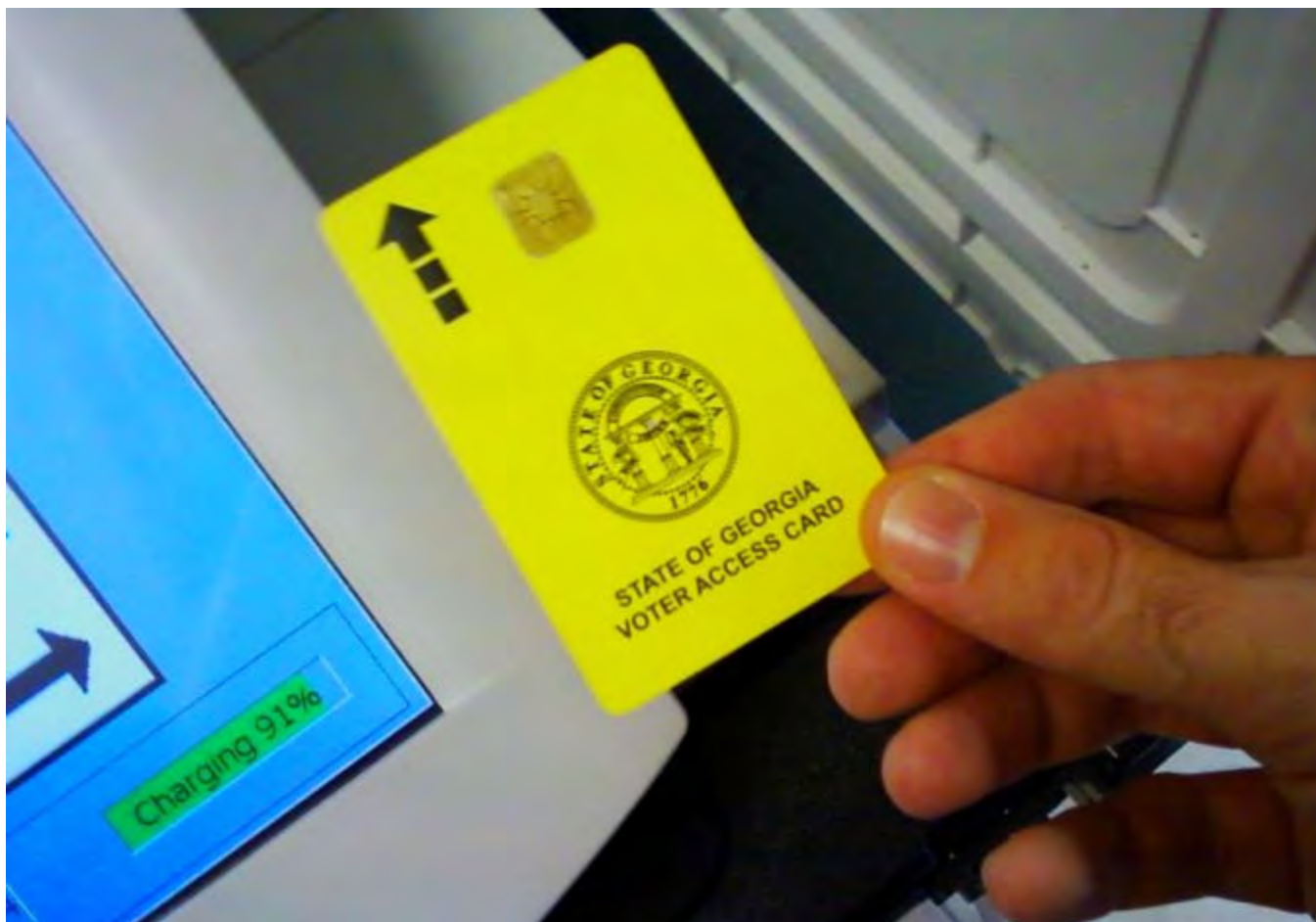
Date: Tuesday, November 20, 2018 at 8:51 AM

To: Marilyn Marks <marilyn@aspenoffice.com>

Subject: Georgia Runoff Will Likely 'Contaminate' Voting Machines As Evidence - WhoWhatWhy

<https://whowhatwhy.org/2018/11/20/georgia-runoff-will-likely-contaminate-voting-machines-as-evidence/>

Georgia Runoff Will Likely 'Contaminate' Voting Machines As Evidence



To vote in person in Georgia, voters have their ballot information downloaded onto a yellow card. That card is then inserted into the Diebold voting machine, the ballot appears on the screen, and the vote can be cast. Errors are common in this system. When Brian Kemp, Republican governor-elect who was also the secretary of state at the time, tried to vote, his initial voter card was rejected as “invalid.” Photo credit: [Jason Riedy / Flickr CC BY 2.0](#))

This week, election officials across Georgia are going to break a rule in the election code and tamper with potential evidence as they prepare for December’s runoff and special elections, just as they have since 2002.

The rule in question mandates the maintenance of the internal memory of voting machines for one month after an election. The problem is that Georgia has an election schedule that makes that rule essentially impossible to enforce. Runoffs, like the one coming up on December 4, often happen within a month of the main election.

WhoWhatWhy investigated whether or not it was possible to both maintain the internal records of voting machines *and* prepare them for use in a new election. Both state and county officials say yes.

Six computer security experts and two lawyers who study election systems disagree.

What's at stake here is more than a scheduling error in Georgia's election code: it is the security and transparency of the election itself.

Why It Matters

.

“The problem with the Georgia system is that you simply don't know,” computer security expert Rich DeMillo said, referring to the legitimacy of an election.

DeMillo, currently a professor of computer science at Georgia Tech, has had a leading role in technology and security at Hewlett-Packard, Bell Communications Research, the National Science Foundation, and the US Department of Defense.

It's a well-established fact that Georgia's election system is vulnerable to cyber attacks [at many levels](#).

It has been public knowledge since at least 2006 that the state's voting machines are vulnerable to hacking.

This is especially troubling since the voting machines do not have a paper trail and cannot be audited. In other words, it's impossible to know with full certainty whether the outcome of any Georgia election actually reflects the votes cast, DeMillo said.

What the state could do — and has never done — is perform a forensic examination of its voting system to search for changes made by an outside party or for irregularities that could have affected the vote.

Messing with the machines or the voter cards is just one way in, but one that has the potential to be extremely effective. By gaining access to just one voting machine, a hacker could modify vote totals for the entire state.

Standing outside of Fulton County's election preparation center, election security expert Logan Lamb explains one of the many ways Georgia's election

could be hacked. Access to just one machine in one county could change votes for the entire state.

Gaining access to a machine is not difficult. *WhoWhatWhy* [found](#) poorly secured voting machines in Fulton County ahead of early voting for this year's midterms, and the "tamper-evident" seals used to lock the machines are easily picked. Once opened, the key to access the memory card slot is commonly available online, or easily picked (it takes under 10 seconds), according to a Princeton University [study](#).

"An attacker who gets physical access to a machine or its removable memory card for as little as one minute could install malicious code," according to that same study.

Logan Lamb, a computer security researcher, shows how easy it is to bypass the "tamper-evident" zip-ties used to seal election machines. Research has shown it takes just over a minute of physical access to download malicious code onto a voting machine.

If votes were to be changed, it could be done in a way that wouldn't be noticed, according to DeMillo. Recounting votes wouldn't catch the error because the votes recorded on each memory card could have been rewritten, and the malicious code could still be in the computers the state uses to count the votes.

Looking at memory cards, or even reading the vote totals saved on the internal memory of DRE machines would likely be ineffective for the same reasons.

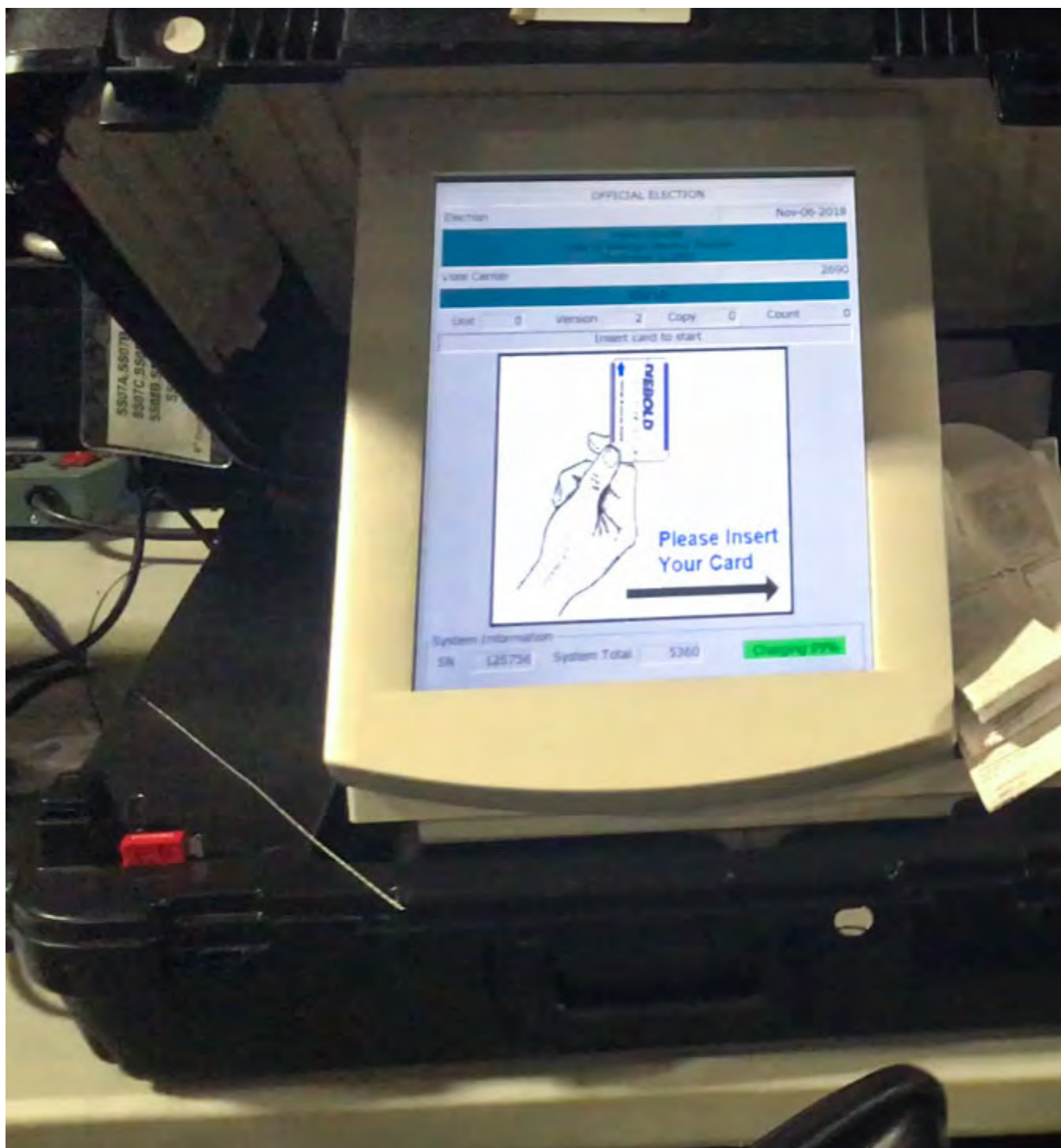
It appears that the best option Georgia has to ensure the accuracy of the election is to perform a forensic audit of the election system, including each voting machine, to search for irregularities or any bad code.

Even if a bad actor were suspected of messing with the election and a forensic examination were to be done (transparently and with opportunity for public review), there is no guarantee that evidence of a hack would be found. It is possible to write malicious code that covers its tracks, so anybody inspecting the machines wouldn't be able to tell that something had been changed.

But the examination is still worth doing, according to DeMillo, because a hacker could make a mistake, be sloppy, or use an attack vector that doesn't affect every machine.

To do that, the state would need to preserve all of the voting machines. The Coalition for Good Governance, currently involved in [litigation](#) against the state for issues of election security, issued a letter to the defendants demanding that they preserve the DREs. If their demand is ignored, the Coalition will take up the issue in court today.

Part of the Coalition's argument is that candidates in the midterms can still contest the election, and that the information on DRE machines should not be changed before they can be reviewed. The letter outlines alternatives for conducting December's election, including using paper ballots.



In front, a voting machine undergoing Logic and Accuracy testing in an election preparation warehouse in Fulton County, GA. Behind, voting machines are sequestered as part of an ongoing election security lawsuit against Fulton County and the secretary of state. Photo credit: Jordan Wilkie / WhoWhatWhy

“It is essential that all November 6 electronic data on the voting machines not be altered by loading runoff ballot programming on the machines,” said Marilyn Marks, the group’s executive director. “Nor should the voting machines be deployed to unsecured locations like polling places. The law and common sense

require that the electronic records be fully and diligently preserved at least until any potential election contests are resolved in the Courts.”

Think of the DREs like evidence in a criminal investigation. If a gun was possibly used in a murder, the police aren’t going to let that gun get wiped down, let it be carried around and left in public places, or allow it to be fired again. That gun will be in a plastic bag in a storage locker until it can get tested for evidence.

State officials knew when they adopted the DRE voting machines in 2002 that they did not have a paper trail. That is the same year that the State Board of Elections wrote a rule, part of the state election code, mandating that the internal memory of voting machines must be maintained for 30 days after an election. That’s the elections version of preserving evidence for an investigation.

Few election officials know about this rule, seem to understand it, or follow it.

The Rule

.

The rule in question is pretty simple. [It reads:](#)

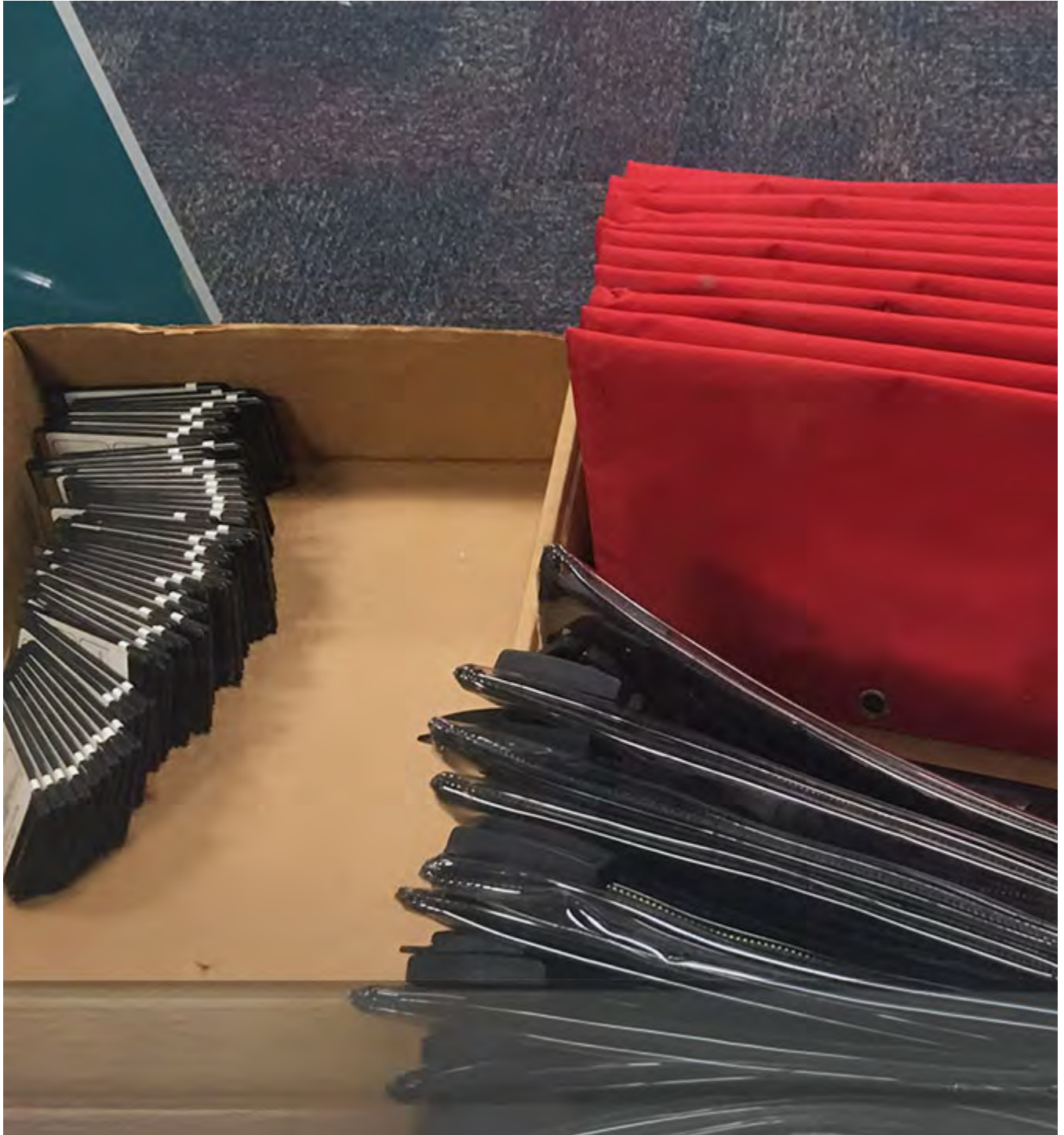
The election results, ballot styles, ballot images, and other information for each election stored in the internal memory storage of each DRE unit shall be maintained for a minimum of one month following each election after which time the results may be erased provided that there are no election contests pending concerning such election.

In summary, data on each DRE used in an election should be preserved for 30 days, and maybe longer if there is an election contest.

But that’s not happening in the real world. Two weeks after Election Day, counties are getting ready to start “Logistics and Accuracy” testing. The state has certified the election and once ballot layouts are finalized (proofs were sent to counties on Saturday), counties will start to program the voting machines for the runoff election.

The question is, how can internal memory be maintained and, at the same time, altered for the new election?

Candice Broce, press secretary for the secretary of state, issued a statement to *WhoWhatWhy*, writing in an email that, “Elections officials comply with this rule in its entirety.”



Memory cards for Diebold DRE voting machines, organized by precinct in Gwinnett County’s election office. Photo credit: Jordan Wilkie / WhoWhatWhy

Matt Bernhard, a computer security expert and Ph.D student in computer science at the University of Michigan, said that, “in computer science terms, this is utter

nonsense, because [the] internal state for a computer changes every time you turn it on.”

To fully preserve the internal memory of a DRE, the machine would need to be stored for a month, with no updating of software, uploading of new ballots, or testing with new memory cards. Just stack the machines in a warehouse and leave them off. Anything else would probably be breaking the rule, if it is read in its strictest sense.

The only possible out, according to Bernhard and other experts, is if the rule is interpreted to only refer to election results, which take up very little space on the memory. Since the oldest files are deleted first, it is very likely — though it cannot be guaranteed — that all of the results from a recent election will be preserved.

Indeed, a statement from Broce suggests that the secretary of state interprets the rule to only include election results.

“Using the machines in a run-off does not affect the storage of previous election results in internal memory,” Broce wrote in an email. “It is false to claim that the only way to preserve data is not to use the machine.”

But that leaves out “ballot styles, ballot images, and other information.” Just looking at election results would not necessarily reveal anything. If a machine had been tampered with, it would store the faulty results, too.

The Legal Take

.

WhoWhatWhy independently consulted with lawyers from two public-interest law firms. Their opinions were consistent. The county election officials are breaking the state’s election rule.

Stacey Leyton, legal partner at Altshuler Berzon, wrote in an email that there were two ways the DREs used in the November 6 election could be used in the December 4 runoff and follow the state’s rule. Neither have been done before, nor are likely now.



Gwinnett County elections office, November 15, 2018, during a recanvass of memory cards requested by citizens to ensure the count was accurate. Stephen Day, the Democratic chairman of the county board of registrations and elections, observes the process. Neither journalists nor poll watchers were allowed access to the room to closely observe the process. Photo credit: Jordan Wilkie / WhoWhatWhy

First, the machines could only be used “if elections officials were able to create an exact image of the internal memory of each voting machine prior to loading the programming for the runoff.”

This process is called mirroring. Its purpose is to capture more information (like the DRE’s programming) more accurately than simply copying the DRE’s memory, according to Camille Fischer, a government transparency lawyer with the Electronic Frontier Foundation.

WhoWhatWhy asked the director of registrations and elections for Fulton County, Richard Barron, if he or his staff knew how to do this.

“We don’t do that,” Barron said, and he doesn’t know how to do it, either. It would either have to be done by the secretary of state’s office or the vendor, he said. *WhoWhatWhy* asked Janine Eveler, director of registrations and elections for Cobb County, the same question and was similarly told that only the machine vendor could make an exact copy of the internal memory of a DRE machine.

Harri Hursti and Logan Lamb, both cybersecurity researchers with expertise in election systems, said this process is onerous. Simply put, it would require soldering a piece of computer hardware to the DRE’s motherboard. Then, a cable would be used to connect the DRE to an external computer and begin downloading. That step alone could take 3–10 hours per machine.

Fulton County alone used almost 2,000 voting machines in the 2018 midterm.

“The alternative, to comply with this rule,” Leyton said, “would be to use paper ballots in the runoff.”

Our Comment Policy

Keep it civilized, keep it relevant, keep it clear, keep it short. Please do not post links or promotional material. We reserve the right to edit and to delete comments where necessary.

EXHIBIT J

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

DONNA CURLING, ET AL.,

Plaintiffs, v.

BRIAN KEMP, ET AL.,

Defendants.

Civil Action No.

1:17-CV-2989-AT

DECLARATION OF RICHARD A. DeMILLO

RICHARD A. DeMILLO (“Declarant”) hereby declares as follows:

1. I am a registered voter in Fulton County Georgia. I am deeply interested in the proper functioning of the Georgia’s voting system from both a personal and professional perspective.
2. I am not a retained expert by any party to this action, but in the desire to aid the Court in the evaluation of technical assertions, I wish to voluntarily offer my opinion on the particular topic of the essential requirements of preservation of electronic records of the DRE voting system including the electronic pollbooks.

3. I am currently the Charlotte B. and Roger C. Warren Chair of Computer Science at Georgia Tech. I have served as Dean of the College of Computing at Georgia Tech and Director of the Georgia Tech Center for Information Security. I have also served as the Chief Technology Officer for Hewlett-Packard, Vice President and General Manager of Computing and Information Research at Bell Communications Research, Director of the Computer and Communications Research Division at the National Science Foundation, and Director of the Software Test and Evaluation Project for the U.S. Department of Defense.
4. In all these appointments, my primary technology focus has been information, communication, cyber security, and computer system testing. I have taught both graduate and undergraduate courses in cyber security, supervised PhD dissertations and conducted peer-reviewed research leading to books, journal articles, patents, and invited addresses, all related to the topic of cyber threats to computer systems. I have served on editorial boards for major journals, chaired program committees for cybersecurity symposia and conferences, and served on government advisory boards and panels. I have been an officer, director, and board member for various public and private corporations in the cyber security industry.

5. I have conducted research and taught courses related to voting system and election security since 2002. I have served as an official observer of foreign electronic voting systems for the Carter Center and participated in the writing of Carter Center guidelines for using electronic voting machines. I serve on the advisory boards of Verified Voting and the Open Software Election Technology Institute.
6. My qualifications and experience are described further in my August 20, 2018 Declaration in this case, Doc. 277 at 52 et seq.
7. I have reviewed the Court's order in this case, as well as the Court's Order in *Common Cause Georgia v. Kemp* (18-cv-5102).
8. I am familiar with Georgia's Diebold DRE voting system, its design, the body of academic literature compiled on the system in the last ten years, and its operation as it is deployed in the polling places in Georgia.
9. I own both Diebold TSx and TS voting machines which I have examined and used to conduct certain experiments related to DRE system security.
10. I have observed the operation of Diebold DRE systems in polling places in multiple Georgia counties over the course of multiple elections and in county election offices where the system was being programmed and tested. I have observed the testing procedures conducted prior to machine deployment to the polling places.

11. I observed the operation of the ExpressPollbooks (electronic pollbooks) as well as the DRE machines in my role as a statewide pollwatcher during the November 6, 2018 election.
12. During my pollwatching activities, I had occasion to speak with voters, election workers, and cybersecurity experts, and to consult various reports. Credible information thus obtained was consistent with the existence of failures and malfunctions of both Diebold ExpressPollbooks operations and DRE voting machines during the November 6, 2018 election.
13. Also, during my pollwatching activities on November 6, 2018, I became aware that certain sites in Gwinnett County were experiencing significant delays in voting and that those delays may have been attributable to malfunctioning Diebold ExpressPollbooks.
14. On the afternoon of November 6, I conferred with nationally recognized Diebold voting systems expert Harri Hursti and cyber security researcher Logan Lamb. This conversation took place a few minutes after Hursti and Lamb completed a review of technical information on site in Anistown Precinct in Gwinnett County, where four-hour voting delays were being attributed to malfunctioning ExpressPollbooks. I visited the Anistown Precinct a few hours after the malfunction had reportedly occurred and

observed the operations at the polling place before visiting other polling locations.

15. I am aware of Election Rule 183-1-12-.02 (6)(d) stating that:

“The election results, ballot styles, ballot images, and other information for each election stored in the internal memory storage of each DRE unit shall be maintained for a minimum of one month following each election after which time the results may be erased provided that there are no election contests pending concerning such election.”

16. One purpose for the requirement for maintaining the information described in Rule (183-1-12-.02(6)(d)) is to make possible forensic analysis in the event of election tampering, system compromise, or system malfunction. This is particularly significant in Georgia because Georgia elections do not create or maintain paper audit trail that can be reviewed as a record of voter intent. Lacking an independent way to judge voter intent, experts need access to the detailed digital records known as footprints (citation: <https://www.nytimes.com/2000/03/09/technology/computer-forensics-teams-learn-to-follow-digital-footprints.html>)

17. The information thus required is not merely a copy of the cast vote records on the machine or ballot images or audit logs, all of which are subject to accidental or malicious corruption, manipulation or destruction during a cyber-attack, system compromise, or system failure, but for all electronic information stored in internal memory. (citation: S. Garfinkel et al, “Practical Unix and Internet Security, 3rd Edition,” O’Reilley Publishing, 2003, pp 677+).
18. Furthermore, merely saving the related memory cards is an inadequate response to this requirement since the very act of copying information from internal memories to memory cards is carried out by software that must be presumed to be untrustworthy in the event of system failure or compromise. (citation: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf) (citation: National Institute of Standards and Technology, Guidelines on PDA Forensics, Special Publication 800-72, November 2004) Additionally, memory cards contain only selected data intended for reporting, not all the operating information on in the DRE internal memory needed for forensic review.
19. Preserving the electronic data in the internal memory of the DRE requires that no new election data be written onto the hard drive of DRE machines,

no further use after the close of the election, including recounts, and that the DRE machines thus preserved be strictly physically secured and not deployed to polling places (see Paragraphs 22 and 23 below).

20. The Election Rule appears to recognize that it is critical that the electronic data in the internal memory of the DRE be preserved for a substantial time in order to permit time for systemic and isolated problems to surface.
21. Therefore, a consequence of Paragraph 19 and the one-month preservation rule is the required availability and use of either alternative DRE machines or paper ballots for elections falling shortly after an election.
22. Preservation of machines identified for analysis is required for this analysis, and therefore all such machines should be removed from service and placed in a secure storage facility, where adequate access and physical safeguards can be implemented to deter tampering. Defendants have represented in prior public statements that election officers already implement secure physical custody. I disagree with this assessment based on well-documented instances in which unattended DREs are easily accessible by persons without authorization or supervision. Defendants have also represented in prior public statements that tamper-evident seals prevent unauthorized access. I disagree with this assessment based on well-known and widely distributed videos that demonstrate how to undetectably defeat

such seals. I have personally observed persons with little or no prior training using shims cut from soft drink cans to defeat the tamper evident seals used in Georgia's elections.

23. Defendants have represented in prior public statements that removal from service is not necessary since data from prior elections cannot be erased, overwritten, or otherwise lost when a new election is carried out. I am unaware of any technical means that would support such a claim. The Windows CE operating system, on which the Diebold Ballot Station software runs, contains only rudimentary memory management and is prone to a phenomenon called memory fragmentation wherein memory locations are not allocated in contiguous blocks but rather are allocated in blocks that are dispersed throughout physical memory. Because Windows CE has no built-in features for signaling to an application that a candidate block of storage has previously been allocated, application software that needs to maintain intact memory from prior elections must carry out the necessary checks. Because Diebold BallotStation software is proprietary and held as a trade secret, it is unavailable for third party evaluation. I have examined various public disclosures that describe the design and coding of BallotStation software. I have not found evidence of such software safeguards in the Diebold BallotStation software.

24. Selection of machines for forensic review during discovery will be done by an algorithm for which section parameters are not yet known and cannot be known until a preliminary analysis has been carried out. For example, one such parameter might be: machines where the polling place manual recap sheet of ballots cast shows a different number than the DRE reported total of ballots cast.
25. All DRE machine electronic data must be preserved. Random sampling of DRE machines for preservation is not sufficient for safe-guarding of electronic evidence required to be used in discovery. Deliberate and time-consuming analysis must first be conducted to determine which DRE machines have exhibited attributes that indicate potential malfunction or have been exposed to greater risk of compromise than others. Randomly sampling the DREs is not a mathematically acceptable way of conducting this analysis. Random sampling assumes an underlying probability distribution for the attributes being tested. A random sample for example might be constructed assuming that defects are uniformly distributed among the DREs. That assumption is untenable since the machines of interest may be associated with certain races, ballots choices, racial distribution, root cause of failure/compromise, geography, population density, number of ballots cast on a machine, voter complaints, anomalous results, or other

attributes that are not uniformly distributed throughout the voting population.

26. Therefore, no statistically valid conclusion can be drawn from a random sample. In addition, statistical tools which might be used to approximate sampling distributions are not applicable in this case, either because the attributes of interest are not statistically independent, or because the software is able to modify its own behavior when it is being tested (as was demonstrated in the Volkswagen emissions testing scandal of 2015 when the US Environmental Protection Agency discovered that on-board software had been programmed to sense when an automobile was being tested and deliver results that did not reflect emissions control impact on vehicle performance. (citation: EPA Notice of Violation September 15, 2015)).

27. Individual imaging of DRE internal memory is technically possible and has been publicly suggested as a way of avoiding preservation. This procedure, however, requires intrusive access to each DRE which makes it an infeasible solution. In the first place, I do not believe there are enough sufficiently trained technicians to accomplish the task. In the second place, it takes anywhere from 3 to 10 hours to obtain an acceptable image of the internal memory of a DRE.

28. The electronic data residing on the components of Georgia's electronic voting systems ("the Required Electronic Data") essential for preservation for the purpose of determining the causes of irregularities and the performance of those systems in the November 6, 2018 General Election follows below in Paragraph 29.

29. The Required Data includes:

- a. all electronic data residing in the internal memory of the DRE machines prepared for use in the November 6, 2018 election, including DRE machines used for uploading memory cards in election offices;
- b. all electronic data on DRE memory cards from all polling places and election offices used in early voting and Election Day voting related to the November 6, 2018 election;
- c. all electronic data residing on the GEMS servers, including logging records and audit logs related to the November 6, 2018 election;
- d. all electronic data residing on external media devices used to upload results to the Election Night Reporting system related to the November 6, 2018 election;
- e. all electronic data residing on Electronic Media Processors related to the November 6, 2018 elections.

f. all electronic data on ExpressPollbooks memory cards used in the November 6, 2018 election.

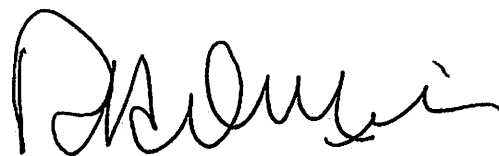
g. all electronic data in the internal memory of the ExpressPollbooks used in the November 6, 2018 election.

h. all electronic data including logging records (including the E-Net systems and vendors' records) used in the upload or download of voter registration records and the electronic pollbooks.

30. As recently as November 17 and 18, I have been made aware of possible anomalies from the November 6 election, and I am aware of various public disclosures of other anomalies. Anomalies such as these would be subject to investigation under the one-month DRE internal memory preservation rule. Investigation of these anomalies would be jeopardized without preservation of the affected DREs.

Pursuant to 28 U.S.C. § 1746, I declare and verify under penalty of perjury that the foregoing is true and correct.

Executed on this date, November 21, 2018.

A handwritten signature in black ink, appearing to read "DeMillo", written in a cursive style.

Richard A. DeMillo

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRIAN KEMP, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

CERTIFICATE OF SERVICE

I hereby certify that on July 25, 2019, a true and correct copy of the foregoing
**COALITION PLAINTIFFS' HEARING BRIEF ON EVIDENTIARY
PRESUMPTION ARISING FROM SPOILIATION OF EVIDENCE** was hand
delivered to all parties.

/s/ Cary Ichter

Cary Ichter