

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF TENNESSEE
CHATTANOOGA DIVISION**

TERPSEHORE MARAS,

Plaintiff,

v.

**REPRESENTATIVE STEVE COHEN, US
DOMINION, INC., DOMINION VOTING
SYSTEMS, INC., DOMINION VOTING
SYSTEMS CORPORATION, MEDIA
MATTERS FOR AMERICA and ALI
ABDUL RAZAQ AKBAR A/KA/ ALI
ALEXANDER,**

Defendants.

Case. No. 1:21-cv-00317-DCLC-CHS

District Judge Clifton L. Corker

Magistrate Judge Christopher H. Steger

**PLAINTIFF TERPSEHORE MARAS' SUPPLEMENTAL BRIEF TO
PLAINTIFF'S MOTION TO COMPEL PRODUCTION OF DOCUMENTS
IDENTIFIED IN NON-PARTY J. ALEXANDER HALDERMAN'S SUBPOENA**

COMES NOW Plaintiff Terpsehore Maras and, by and through undersigned counsel and pursuant to LR7.01(d), hereby files Plaintiff Terpsehore Maras' Supplemental Brief to Plaintiff Terpsehore Maras' Supplemental Brief to Plaintiff's Motion to Compel Production of Documents Identified in Non-Party J. Alexander Halderman's Subpoena, and Plaintiff respectfully shows unto this Honorable Court the following:

**I. THE HALDERMAN REPORT IS NECESSARY AS CORROBORATING
EVIDENCE THAT WILL BE USED IN PLAINTIFF'S CASE IN CHIEF IN
PROVING HER DEFAMATION CASE AGAINST THE DEFENDANTS.**

After Plaintiff filed her Motion to Compel Production of Documents Identified in Non-Party J. Alexander Halderman's Subpoena, new information was obtained regarding the apparent election fraud in the 2020 elections. The Plaintiff is a former private intelligence contractor, a whistleblower

and an investigative journalist seeking to remedy the damages to her reputation due to the statements of libel/defamation made by the Defendants. While Dr. J. Alexander Halderman's purported lawyer (David Cross) did not initially object to being counsel for Dr. Halderman, Mr. Cross now objects to being counsel for Dr. Halderman. *See* Exhibit A, E-mail Correspondence from David Cross. As such, Plaintiff's Certificate of Service will be updated to serving Dr. Halderman at his last known address.

As an investigative journalist, Plaintiff has confidential sources that have provided her with both the public seven page summary and a non-public unredacted twenty-four-page summary of the Halderman Report that she has obtained from sources that are protected, as they are privileged and confidential. *See* Exhibit B, September 21, 2021, Declaration of J. Alexander Halderman; *see* Exhibit C, August 2, 2021 Declaration of J. Alexander Halderman. As the court can see, both of Dr. Halderman's reports directly relate to matters contained in Plaintiff's Affidavit, which forms the basis and impetus of the Defendants' defamation. The Plaintiff presented evidence of election fraud in her affidavit and she now needs Dr. Halderman's full unredacted twenty-five-thousand-word report to use as corroborating evidence in proving her defamation case in chief against the Defendants.

Both of Dr. Halderman's election fraud declarations, which are summaries of his details reports and they are proof positive of election fraud, which expressly named the Dominion equipment. Dr. Halderman's Declarations show different perspectives and aspects of the severe vulnerabilities that demonstrate that the right to vote by citizens is unprotected when using Dominion Voting machines. In her Affidavit, Plaintiff testified that vulnerabilities from COTS (components off the shelf) as Shellshock¹ and patch management systems in place are still vulnerable to domestic and foreign hacking and it was made public. Thus far, Georgia's Center for Election Systems were found to have **not** had a patch in either 2016 or 2018. *See* Exhibit D, Georgia election systems could have

¹ Shellshock is a vulnerability that allows systems containing a vulnerable version of Bash to be exploited to execute commands with higher privileges. This allows attackers to potentially take over that system.

been hacked before 2016 vote, <https://www.politico.com/news/2020/01/16/georgia-election-systems-could-have-been-hacked-before-2016-vote-100334> (last visited March 17, 2022).

In fact, Dr. Halderman's two Declarations regarding election fraud concur with Plaintiff's Affidavit and her testimony regarding the COTS (components off the shelf) vulnerabilities. Many states have ignored the patch vulnerabilities of COTS and many state and/or electronic voting systems remain unpatched and are compromised (knowingly or unknowingly), despite the repeated Department of Homeland Security alerts that were sent out to states. This compromise makes the states and/or electronic voting systems vulnerable to Shellshock, which means that the electronic voting machines are at a continuous state of vulnerability to domestic and/or foreign hacking. In addition, it is public knowledge that Georgia's Center for Election Systems were determined to be vulnerable from even before the 2016 elections, which concurs with Plaintiff's sworn testimony of ongoing long standing voting integrity concerns. *See* Exhibit D.

II. ARGUMENT AND CITATION OF AUTHORITY

Pursuant to Local Rule 7.1(d),

Supplemental Briefs. No additional briefs, affidavits, or other papers in support of or in opposition to a motion shall be filed without prior approval of the Court, **except that a party may file a supplemental brief of no more than 5 pages to call to the Court's attention developments occurring after a party's final brief is filed.** Any response to a supplemental brief shall be filed within 7 days after service of the supplemental brief and shall be limited to no more than 5 pages.

Local Rule 7.1(d) (emphasis added).

In the case at bar, this Court should compel Dr. Halderman to produce his full and unredacted Report because it contains corroborating sworn testimony regarding election fraud that Plaintiff needs in order to prove her defamation case against the Defendants. Dr. Halderman's

Report on the election fraud is not privileged. Dr. Halderman's report is discoverable. Plaintiff needs this report as corroborating evidence in order to prove her election fraud case.

Respectfully submitted this *17th* day of March, 2022.

THE NEWMAN LAW FIRM

/s/ Russell A. Newman
Russell A. Newman, BPR No. 033462
6688 Nolensville Road
Suite 108-22
Brentwood, TN 37027
(615) 554-1510 (Telephone)
(615) 283-3529 (Facsimile)
E-mail: russell@thenewmanlawfirm.com
Attorney for Plaintiff Terpsehore Maras

CERTIFICATE OF SERVICE

I, Russell A. Newman, do hereby certify that I am counsel for Plaintiff Terpsehore Maras in the above-captioned matter and that a copy of the **PLAINTIFF TERPSEHORE MARAS' SUPPLEMENTAL BRIEF TO PLAINTIFF'S MOTION TO COMPEL PRODUCTION OF DOCUMENTS IDENTIFIED IN NON-PARTY J. ALEXANDER HALDERMAN'S SUBPOENA** was filed and served via the CM/ECF system for the United States District Court, Eastern District of Tennessee, Chattanooga Division via electronic mail to the following CM/ECF filers:

W. Scott Sims, Esq.
Michael R. O'Neill, Esq.
Sims | Funk, PLC
3322 West End Ave., Suite 200
Nashville, TN 37203
(615) 292-9355 (Telephone)
(615) 649-8565 (Facsimile)
ssims@simsfunk.com
moneill@simsfunk.com
Attorneys for Dominion Defendants

Robb Harvey, Esq.
511 Union Street, Suite 2700
P.O. Box 198966
Nashville, TN 37219-8966
Robb.harvey@wallerlaw.com

Todd B. Tatelman, Esq.
Sarah Clouse, Esq.
5140 O'Neill House Office Building
Washington D.C. 20515
Todd.tatelman@mail.house.gov
Sarah.clouse@mail.house.gov
Attorneys for Congressman Steve Cohen

Moziano S. Reliford, Esq.
William J. Harbison, II, Esq.
1201 Demonbreun Street, Suite 1000
Nashville, TN 37213
treliford@nealharwell.com
jharbison@nealharwell.com
Attorneys for Defendant Media Matters for America

And via E-Mail on the following non-registered CM/ECF filers:

Baron Coleman, Esq.
Three South Jackson Street
P.O. Box 789
Montgomery, AL 36101-0789
baron@baroncoleman.com
Attorney for Defendant Ali Abdul Razaq Akbar

And via U.S. Mail on the following non-registered CM/ECF filers:

Dr. J. Alexander Halderman
632 N 4th Ave.
Ann Arbor, MI 48104

Respectfully submitted this *17th* day of March, 2022.

THE NEWMAN LAW FIRM

By: /s/ Russell A. Newman
Russell A. Newman, BPR # 033462

Subject: RE: Halderman Subpoena: Curling v. Raffensperger

Date: Wednesday, March 16, 2022 at 10:47:01 Central Daylight Time

From: Cross, David D.

To: Russell Newman

Mr. Newman -

I received a hardcopy by regular mail of a motion to compel it appears you have filed against Dr. Halderman in your case. It's unclear why you did not send a courtesy copy by email given we have corresponded by email regarding the subpoena. You also must know that these days folks often are not in the office given many business facilities remain closed with employees working remotely.

In any event, you have not properly served your motion. I did not agree to accept service of the motion on behalf of Dr. Halderman, nor did you ask that I do so. I also do not have authority for him to do that. If you intend to pursue this motion, you need to effect proper service. Please confirm that you will let the court know that the motion has not been served.

I once again encourage you to withdraw this motion and not to pursue the subpoena. Your motion misstates the law and is completely lacking in merit. I also understand that the court has not yet authorized discovery to begin in your case, which makes the subpoena and the motion doubly improper. Please understand that we will seek all fees and costs associated with this subpoena if you persist given its obvious impropriety and the frivolousness of your pursuit in light of the order from Judge Totenberg prohibiting Dr. Halderman from disclosing the report you seek.

Best,
DC

From: Cross, David D. <DCross@mofo.com>

Date: Monday, Feb 14, 2022, 10:56 PM

To: Russell Newman <russell@thenewmanlawfirm.com>

Subject: RE: Halderman Subpoena: Curling v. Raffensperger

Mr. Newman -

The Court repeatedly has ordered the parties and Dr. Halderman not to disclose the report to third parties. It also has repeatedly denied motions by third parties filed in our case for a copy of the report, just as you're seeking. Judge Totenberg's orders are publicly available on the docket in our case.

What authority do you have that one federal judge can order disclosure of something another federal judge has ordered not to be disclosed? You fundamentally misunderstand the jurisdiction of federal courts which is national, not regional as you wrongly posit — which is of course why courts can and often do enter injunctions and other orders that apply across the US, not just in a particular district or circuit.

Again, if you make us brief this in your court, we'll seek fees and costs and any other appropriate relief. A motion to compel would be utterly frivolous.

Best,
DC

From: Russell Newman <russell@thenewmanlawfirm.com>
Date: Monday, Feb 14, 2022, 7:28 PM
To: Cross, David D. <DCross@mofo.com>
Subject: Re: Halderman Subpoena: Curling v. Raffensperger

External Email

Good evening, Mr. Cross.

Thank you for your e-mail. We will direct future correspondence to you as counsel for Dr. Alex Halderman as it relates to Plaintiff's subpoena.

Plaintiff intends to move forward by filing a motion to compel, but before doing so I wanted to have a brief conversation with you in a good faith effort to amicably resolve our dispute without involving our judge. Plaintiff contends that the Northern District of Georgia, Atlanta Division does not have subject matter jurisdiction over the Eastern District of Tennessee, Chattanooga Division. Even at the appellate level, we are in Sixth Circuit Court of Appeals and the Curling case is in the Eleventh Circuit Court of Appeals. As such, neither the district court nor court of appeals have subject matter jurisdiction over our court. Could you please share with us the authority that you are relying on to withhold production of otherwise discoverable items?

Kindly provide us with a response as soon as possible, but in any event please do so by the close of business on Wednesday (02/16/22). In advance, thank you for your consideration of this matter.

Best regards,

Russell A. Newman, Esq.

The Newman Law Firm

6688 Nolensville Road

Suite 108-22

Brentwood, TN 37027

T: [\(615\) 554-1510](tel:(615)554-1510)

F: [\(615\) 283-3529](tel:(615)283-3529)

Email: russell@thenewmanlawfirm.com

<https://www.thenewmanlawfirm.com/>

CONFIDENTIALITY NOTICE: This e-mail communication, including any attached files was sent by or on behalf of the firm and may contain entity to which it is addressed. If you are not the intended recipient or the person responsible for delivering this Communication to the intended recipient, please immediately notify the sender via return email or telephone.

On Mon, Feb 14, 2022 at 1:09 PM Cross, David D. <DCross@mofo.com> wrote:

Mr. Newman –

Please see the attached correspondence.

Best,

DC

DAVID D. CROSS

CHAIR OF ANTITRUST LITIGATION PRACTICE

Partner | Morrison & Foerster LLP

2100 L Street, NW, Suite 900 | Washington, DC 20037

P: +1 (202) 887-8795

mofo.com | [LinkedIn](#) | [Twitter](#)

=====

This message may be confidential and privileged. Use or disclosure by anyone other than an intended addressee is prohibited. If you received this message in error, please delete it and advise the sender by reply email. Learn about Morrison & Foerster LLP's [Privacy Policy](#).

=====

This message may be confidential and privileged. Use or disclosure by anyone other than an intended addressee is prohibited. If you received this message in error, please delete it and advise the sender by reply email. Learn about Morrison & Foerster LLP's [Privacy Policy](#).

EXHIBIT A

**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.**

**DECLARATION OF
J. ALEX HALDERMAN**

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

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. My July 1, 2021, expert report describes numerous security vulnerabilities in Georgia's Dominion ICX BMDs. These include flaws that would allow attackers to install malicious software on the ICX, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. They are not general weaknesses or theoretical problems, but

rather specific flaws in the ICX software, and I am prepared to demonstrate proof-of-concept malware that can exploit them to steal votes cast on ICX devices.

3. Some of these critical vulnerabilities could be at least partially mitigated through changes to the ICX software if Dominion implemented such changes and jurisdictions deployed them. However, it would likely take months for Dominion to assess the problems, develop responsive software updates, test them, obtain any necessary approvals from the EAC and state-level certification authorities, and distribute the new software to states, as well as additional time for localities to install the changes. But Dominion cannot begin this process, because (to my knowledge) they have yet to learn what is in my report.

4. My analysis also concludes that the ICX is very likely to contain other, equally critical flaws that are yet to be discovered. Jurisdictions can mitigate this serious risk through procedural changes, such as reserving BMDs for voters who need or request them. Election officials cannot make an informed decision about such urgent policy changes or any other mitigations until they have assessed the technical findings in my report. However, to my knowledge, the Georgia Secretary of State's Office has yet to even request access to it, despite Plaintiffs' repeated offers to make it available to appropriate individuals at the Secretary's Office.

5. Nor do these problems affect Georgia alone. In 2022, the ICX will be used in parts of 16 states.¹ Nevada will use it as the primary method of in-person voting in certain areas of the state. Louisiana is slated to use it for early voting in a DRE configuration where there is not even a paper trail. It will be used for accessible voting in Alaska and large parts of Arizona, California, Colorado, and Michigan. It will also see some use in parts of Illinois, Kansas, Ohio, Missouri, New Jersey, Pennsylvania, Tennessee, and Washington State. Officials in these jurisdictions too must act to update the software and their procedures, but they cannot do so without information about the problems. Continuing to conceal those problems from those who can—and are authorized to—address them, to the extent possible, serves no one and only hurts voters (and heightens the risk of compromise in future elections).

6. The most effective way to ensure that the necessary information gets to the parties responsible (without also falling into the wrong hands) would be to share my report with the Cybersecurity and Infrastructure Security Agency (CISA), which operates a Coordinated Vulnerability Disclosure (CVD) program for just this purpose. CISA is a federal agency that collaborates with state and local governments, election officials, federal partners, and vendors to manage risks to U.S. election

¹ See Verified Voting, “Verifier Search – November 2022,” <https://verifiedvoting.org/verifier/#mode/search/year/2022/model/ImageCast%20X>.

infrastructure.² Under CISA's CVD process, agency staff would independently validate the vulnerabilities, work with Dominion to develop software updates as necessary, and facilitate sufficient time for affected states and localities to apply mitigation strategies.³ CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary,"⁴ making it well qualified to coordinate the disclosure of such sensitive vulnerabilities.

7. Geoff Hale, Director of CISA's Election Security Initiative, has confirmed to me that, if the Court permits it, the agency would be willing to receive my expert report and carry out coordinated vulnerability disclosure activities as appropriate (see Exhibit 1). Mr. Hale requests that I and my assistant Drew Springall be available for consultation with CISA during the CVD process, which we would be willing to do subject to the Court's permission.

8. Informing responsible parties about the ICX's vulnerabilities is becoming more urgent by the day. Foreign or domestic adversaries who are intent on

² Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Initiative," <https://www.cisa.gov/election-security>.

³ Cybersecurity and Infrastructure Security Agency, "Coordinated Vulnerability Disclosure Process," <https://www.cisa.gov/coordinated-vulnerability-disclosure-process>.

⁴ *Id.*

attacking elections certainly could have already discovered the same problems I did, yet Georgia's 2022 primaries are less than nine months away, and other states that use the ICX will conduct high-profile elections even sooner. It is important to recognize the possibility that nefarious actors already have discovered the same problems I detail in my report and are preparing to exploit them in future elections. Providing my report to CISA through its CVD program will ensure that Dominion and affected jurisdictions are able to begin appropriate mitigations as soon as possible. Continuing to withhold my report from CISA puts voters and election outcomes in numerous states at unnecessary, and avoidable, risk.

9. I understand that State Defendants object to disclosure to CISA on the argument that my report should be used only for this lawsuit. But this ignores the implications of my report and my role in this matter. I am not a party to this lawsuit. I am an independent expert who was engaged to conduct an impartial assessment of the security and reliability of the Dominion BMD system, using (in part) election equipment that the Court ordered I be provided. I have done that, as reflected in my lengthy, detailed report and other submissions in this matter. As an independent expert and member of the election integrity community, I have a professional obligation to take appropriate steps to ensure that the severe vulnerabilities my report describes are properly remediated, to the extent possible, and that those tasked with

election security and administration across the country have the information they need to make responsible, informed decisions about election procedures, including the equipment used, the manner and purposes for which it is used (including whether it is used at all), the steps needed to secure that equipment and other aspects of the election systems in which it is used, and more. In short, my professional obligations do not end at the boundaries of this lawsuit, nor do the serious risks to voters and elections that my report discusses in depth. Additionally, I can imagine no prejudice to anyone in this lawsuit (or beyond) from disclosure of my report to CISA, nor am I aware of any claim of prejudice from any of the parties.

10. I of course have complied, and will continue to comply, with all directives from the Court regarding disclosure of my work in this matter. I submit this declaration to explain why I believe disclosure of my report to CISA is critically important (and not just for Georgia) and to respectfully ask that the Court allow that disclosure, rather than accept State Defendants' position that my findings must not be shared beyond the confines of this lawsuit, including with those who are authorized to address the vulnerabilities with the ICX and stand ready to do so. If my findings regarding the ICX actually present no meaningful risks to voters and election outcomes and therefore require no remediation, as I gather State Defendants would have the Court believe, CISA is well positioned to determine that. If, on the other

hand, my findings do warrant remediation, as I believe they do, then CISA is well positioned to work with Dominion and the appropriate authorities around the country to implement remedial measures. I can see no reason to prevent (or further delay) that important work for future elections. And I note that none of State Defendants' experts have disputed my findings regarding the ICX machines. Only Dr. Juan Gilbert has responded to my sealed report, and he has not examined the machines (or used them) to my knowledge.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 21st day of September, 2021 in Ann Arbor, Michigan.



J. ALEX HALDERMAN

EXHIBIT 1



J. Alex Halderman <halderman@gmail.com>

Vulnerability Disclosure

Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>
To: "J. Alex Halderman" <jhalderm@umich.edu>
Cc: Andrew Springall <andrew.springall@gmail.com>

Thu, Aug 19, 2021 at 12:15 PM

Prof. Halderman,

Thank you for your email. Yes, CISA would be willing to receive the report regarding possible vulnerabilities in election infrastructure for inclusion in CISA's Coordinated Vulnerability Disclosure (CVD) process and would carry out any further coordinated disclosures activities as appropriate. As we share on our public website (<https://www.cisa.gov/coordinated-vulnerability-disclosure-process>), CISA's CVD program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). Note that part of our process may also involve validating any alleged vulnerabilities, planned mitigations, remediations, or patches with the security researcher who discovered the alleged vulnerability, so we would appreciate if you could continue to be available for consultation during the CVD process as well.

As shared on our website, please submit any vulnerability reports for CVD coordination using the form here:
<https://www.kb.cert.org/vuls/report/>

Best,

Geoff

From: J. Alex Halderman <jhalderm@umich.edu>
Sent: Wednesday, August 18, 2021 4:37 PM
To: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>
Cc: Andrew Springall <andrew.springall@gmail.com>
Subject: Vulnerability Disclosure

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Dear Mr. Hale,

We are writing to you in your capacity as Director of the Election Security Initiative at the federal Cybersecurity and Infrastructure Security Agency (CISA).

We understand that the Election Security Initiative at CISA works to ensure the physical security and cybersecurity of the systems and assets that support the Nation's elections, including through detection and prevention, information sharing and awareness, and incident response.

As you may be aware from recent press reports, one of us (Halderman) is presently serving as an expert witness for the plaintiffs in *Curling v. Raffensperger* (Civil action no. 1:17-CV-2989-AT, N.D. Ga.), a case that concerns the security of Georgia's election system. A year ago, the court granted plaintiffs access to an ICP ballot scanner and ICX ballot marking device as used in Georgia in order to test their security. Following months of analysis, on July 1, Dr. Halderman submitted an expert report that describes several very serious vulnerabilities we found in the equipment, which, to our knowledge, have not been previously documented or disclosed.

Given the nature of the vulnerabilities and the time that would be necessary to mitigate them before the 2022 midterm elections, we believe it is critical for Dominion and affected jurisdictions (which include Georgia and parts of many other states) to begin taking responsive action soon. It is also vitally important to prevent information sufficient to exploit the vulnerabilities from falling into the wrong hands, and to avoid fueling election-related misinformation if possible.

Currently, disclosure of the expert report to anyone other than outside litigation counsel for the parties is strictly prohibited by the Court's protective order and by recent directives from the judge. However, if permitted by the Court, we would like to share the report with CISA and ask your agency to carry out appropriate further disclosure of the information it contains to Dominion and affected jurisdictions as you see fit, under CISA's coordinated vulnerability disclosure (CVD) program (<https://www.cisa.gov/coordinated-vulnerability-disclosure-process>).

We understand that under this process, CISA will work with the vendor (Dominion) for mitigation development and the issuance of patches or updates and to facilitate sufficient time for affected end users to obtain, test, and apply mitigation strategies. We further understand that CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary".

Please confirm that CISA would be an appropriate agency to handle coordinated vulnerability disclosure for election infrastructure under these circumstances, and that you would be willing to receive the report (subject to the Court's permission) and carry out further disclosures as you deem appropriate.

Sincerely,

J. Alex Halderman

Drew Springall

**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.**

**DECLARATION OF
J. ALEX HALDERMAN**

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

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. I have reviewed the expert disclosures prepared by Dr. Juan Gilbert and Dr. Benjamin Adida for State Defendants. Neither Dr. Gilbert nor Dr. Adida offers any rebuttal to the numerous, critical vulnerabilities in Georgia's BMDs that I described in my July 1, 2021 expert report. Dr. Adida did not respond to my report at all; State Defendants reissued prior declarations from him previously provided in this litigation. Neither of them disputes the presence of any of the serious

vulnerabilities I detail in my report or the steps I describe for exploiting those vulnerabilities to alter individual votes and election outcomes in Georgia. Nor does either of them claim to have examined any of the voting equipment used in Georgia to evaluate whether the vulnerabilities I identified—or others—have been exploited in any past election. Although each of them presumably could do this with the permission of State Defendants, who I understand engaged them as experts in this case, there is no indication either has undertaken any such inquiry or asked to do so. As a result, neither Dr. Gilbert nor Dr. Adida has anything to say about the reliability of the voting equipment used in Georgia elections. This is surprising, given that they have had at least the last year to examine Georgia's voting equipment.

3. State Defendants urgently need to engage with the findings in my report and address the vulnerabilities it describes before attackers exploit them. Nothing in Dr. Gilbert's or Dr. Adida's responses indicates that State Defendants understand the seriousness of these problems or have taken any measures to address them and their implications for the Plaintiffs' individual votes in future elections. Established practice in the security field would require State Defendants to promptly subject Georgia's voting system to rigorous testing in response to my report, to assess the extent and significance of each of the vulnerabilities I described, and to identify and *promptly implement* specific measures (where possible) to eliminate or mitigate each

of those vulnerabilities. Neither Dr. Gilbert nor Dr. Adida indicates any such efforts on their own part or on the part of State Defendants or anyone else. Again, Dr. Adida did not respond to my report.

4. In my report—a 25,000-word document that is the product of twelve weeks of intensive testing of the Dominion equipment provided by Fulton County—I find that Georgia’s BMDs contains multiple severe security flaws. Attackers could exploit these flaws to install malicious software, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. I explain in detail how such malware, once installed, could alter voters’ votes while subverting all the procedural protections practiced by the State, including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs). Finally, I describe working proof-of-concept malware that I am prepared to demonstrate in court.

5. My report concludes, *inter alia*, that Georgia’s BMDs are not sufficiently secured against technical compromise to withstand vote-altering attacks by bad actors who are likely to target future elections in the state; that the BMDs’ vulnerabilities compromise the auditability of Georgia’s paper ballots; that the BMDs can be compromised to the same extent as or more easily than the DREs they replaced; and that using these vulnerable BMDs for all in-person voters, as Georgia

does, greatly magnifies the level of security risk compared to using hand-marked paper ballots and providing BMDs to voters who need or request them.

Reply to Declaration of Dr. Juan Gilbert

6. Rather than engage with the facts in my report, Dr. Gilbert responds largely with vague generalities. He gives no indication that he has ever used an ICX BMD, let alone tested its security. He begins by conceding that “any computer can be hacked,” but he contends that “this general statement is largely irrelevant,” because hand-marked paper ballot systems use computers too (to scan the ballots) (§ 6). His position is inconsistent with accepted standards for election security and with the facts of the particular voting system used in Georgia.

7. My testing has shown that the BMDs used in Georgia suffer from specific, highly exploitable vulnerabilities that allow attackers to change votes despite the State’s purported defenses. There is no evidence that Georgia’s ballot scanners suffer from the same extraordinary degree of exploitability, nor does Dr. Gilbert contend they do. He ignores the relative ease with which Georgia’s BMDs can be hacked, including by a voter in a voting booth in mere minutes. That extreme difference in security as compared to other voting technologies, particularly hand-marked paper ballots, is far from “irrelevant” as Dr. Gilbert implies.

8. Furthermore, even if the scanners were just as insecure as the BMDs, Georgia's practice of requiring essentially all in-person voters to use highly vulnerable BMDs would needlessly give attackers *double* the opportunity to change the personal votes of individual Georgia voters, since malware could strike either the BMDs or the scanners. Accepted standards in election security compel reducing points of attack for bad actors, not unnecessarily expanding them—a point Dr. Gilbert ignores.

9. Lastly, Dr. Gilbert also ignores that accepted election security protocols include an effective measure to protect against hacks of ballot scanners when the ballots are hand-marked rather than generated by BMDs—namely, reliable risk-limiting audits (RLAs), which would have a high probability of detecting any outcome-changing attack on the scanners. Not only do Georgia's BMDs defeat the efficacy of RLAs, but Dr. Gilbert continues to ignore the fact that Georgia requires an RLA of just one statewide contest every two years (and, to my knowledge, has not adopted specific, adequate procedures to ensure a reliable RLA for that one audit every other year).

10. Dr. Gilbert goes on to discuss issues related to voter verification of BMD ballots (which I respond to below). Yet he fails to address the potential for attackers to cheat by changing only the QR codes printed by Georgia's BMDs.

Voters cannot read the QR codes, but they are the only part of the ballots that the scanners count. My report details several routes by which malicious hardware or software can manipulate the QR codes and cause the recorded votes to differ from voters' selections. In principle, a rigorous risk-limiting audit would be likely to detect such an attack if the attacker changed enough votes to alter the outcome of the contest being audited, but again Georgia rules require such an audit in only a single statewide contest once every two years. As my report explains, this leaves the vast majority of elections and contests in Georgia vulnerable to QR code (and others) attacks, yet Dr. Gilbert says nothing about this threat.

11. Instead, Dr. Gilbert focuses exclusively on a different threat: attacks that change *both* the QR codes and the ballot text. In addition to the barcode-only attacks I just discussed, my report demonstrates that Georgia's BMDs can be manipulated so that both the barcodes and the printed text indicate the same fraudulent selections. No audit or recount can catch such fraud, because all records of the voter's intent would be wrong. The only reliable way to detect it would be if enough voters carefully reviewed their ballots, noticed that one or more selections differed from their intent, and reported the problems to election officials, *and* if Georgia officials then discerned from the pattern of voter reports that the BMDs were systematically misbehaving. Thus, Dr. Gilbert is mistaken when he contends that the distinction

between “voter-verifiable” and “voter-verified” paper ballots “only matters in principle” (§ 7). All BMD ballots are potentially voter-verifiable, but unless enough BMD ballots are actually voter-*verified*, BMD-based attacks could alter election outcomes even in the rare instances where the State conducts a risk-limiting audit. And unless *every* BMD ballot is actually voter-*verified*, BMD-based attacks could alter individual voters’ selections without detection..

12. A large body of recent scientific evidence has established that few voters are likely to catch errors caused by malicious BMDs. I have reviewed this evidence in previous declarations.¹ It comes from both field observations (which report how long real voters review their ballots during real elections) and laboratory tests (which report the fraction of errors that subjects detect when voting on hacked BMDs in simulated elections). These methodologies are complementary, and results to-date from all studies of both kinds point to a low rate of voter-verification.

13. Dr. Gilbert criticizes field observations because “[t]ime spent reviewing a ballot has little to do with whether it was actually verified” (§ 9). This claim is inconsistent with accepted election security principles. Of course, they are not exactly the same question, but obviously the time spent reviewing a ballot can

¹ *Halderman decl.* (Dec. 16, 2019), Dkt. 682 at 23-33; *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 6-8, 55.

provide important insight into whether it was likely verified. For example, we can conclude that a voter who spends only a second or two reviewing a lengthy, complicated ballot is unlikely to have reliably verified each of their selections on the ballot. And of course, the same is true for a voter who spends no time at all reviewing their ballot. Review time is both practical to measure and clearly correlated with the error detection success, making it a valuable and relevant metric, as multiple studies confirm.

14. Dr. Gilbert seems to contend, without evidence, that a casual glance is sufficient to review Georgia-style ballots because selections are printed together with party affiliations (§ 9). He cites no research (and I am unaware of any) that supports this conclusion, particularly when, as in Georgia, the party affiliations are printed in small type and in a different horizontal position for each contest. A real BMD ballot is reproduced on page 15 of my expert report. This is just one example of such a ballot; they can be longer and more confusing. Dr. Gilbert provides no basis for believing that voters would likely catch deliberate errors caused by compromised BMDs when voting such a ballot.

15. Dr. Gilbert references my award-winning peer-reviewed study about voter verification behavior, which found very poor rates of error detection and

reporting in a mock election using BMDs that my team hacked (§ 10).² He contends that my study “ignores the reaction to such manipulation in an actual election, particularly one as heated in the public domain as the 2020 Election.” (§ 11). He does not explain how or why such circumstances would be expected to materially increase voter verification of their respective BMD ballots, nor does he cite any support for his claim to believe they would. And, just last week, the Atlanta Journal-Constitution obtained a study (under the Georgia Open Records Act) commissioned by the Secretary of State’s Office in which researchers from the University of Georgia observed Georgia voters during the November 2020 election and reported how long they spent reviewing their BMD ballots.³ Although it appears the Secretary of State had this study at the time of Dr. Gilbert’s response to my report, he does not address or acknowledge it. The new study suggests that voters in the real world review their ballots *even less carefully* than voters in recent laboratory studies—despite the reminders election workers are supposed to give them to carefully review

² Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, “Can Voters Detect Malicious Manipulation of Ballot Marking Devices?” In *41st IEEE Symposium on Security and Privacy* (May 2020). Available at <https://ieeexplore.ieee.org/document/9152705>.

³ Mark Niesse, “Under half of Georgia voters checked their paper ballots, study shows,” *Atlanta Journal-Constitution* (July 27, 2021). Available at <https://www.ajc.com/politics/under-half-of-georgia-voters-checked-their-paper-ballots-study-shows/6HSVHHFOBRBDPODRZXLIBTUS64/>.

their ballots at the polling sites, which Dr. Gilbert emphasizes as a remedy for poor voter verification of BMD ballots.⁴

16. The University of Georgia researchers report that 20% of voters they observed did not check their ballots at all.⁵ Only about 49% examined their ballots for at least one second, and only 19% did so for more than five seconds. This is significantly worse performance than observed in my study, which found that when voters were verbally prompted to review their ballots before casting them, as should occur in Georgia, 63% of voters reviewed their ballots for only *two* seconds or more, compared to 19-49% in the new study.

17. This suggests that laboratory studies like mine tend to *overestimate* the rate at which real Georgia voters would detect errors on their BMD ballots. Since real Georgia voters were observed to review their ballots even less carefully than the

⁴ Secretary Raffensperger appears to disagree with Dr. Gilbert about the value of measuring voter review time for assessing voter verification performance. He told the Atlanta Journal-Constitution that the new study “shows voters do indeed review their ballots for accuracy before casting them” and offers “proof the votes that were counted were for the candidates the voters intended.” (*Id.*). I agree that the new study provides valuable insights about voter behavior, but, contrary to the Secretary’s pronouncements, the results indicate that real Georgia voters are even less likely to detect errors caused by compromised BMDs than previous studies have suggested.

⁵ Audrey A. Haynes and M.V. Hood III, “Georgia Voter Verification Study” (January 22, 2021). Available at <https://s3.documentcloud.org/documents/21017815/gvvs-report-11.pdf>.

participants in my study, it is reasonable to infer that real voters would catch an even smaller fraction of errors. The participants in my study who were similarly prompted to review their ballots caught 14% of errors. Therefore, real voters in Georgia are likely to catch substantially less than 14% of errors.

18. How often would voters have to detect errors on their BMD ballots to effectively safeguard against attacks? The answer depends on the margin of victory, since an outcome-changing attack would need to change fewer votes in a close contest. The model from my study shows that, given the margin of victory from the 2020 Presidential contest in Georgia, voters would need to have detected 46% of errors for there to be even one error report per 1000 voters, under a hypothetical scenario where the election outcome had been changed by hacked BMDs.⁶ The University of Georgia observations show that barely 49% of voters looked at their ballots for even a second, let alone studied them carefully enough to reliably spot errors.

⁶ To reiterate, the November presidential race was the only state-wide contest subjected to a risk-limiting audit. In other contests, attackers could change the outcome by tampering with only the ballot QR codes, and voters would have no practical way to detect this manipulation regardless of how diligently they reviewed their ballots.

19. Dr. Gilbert performs a similar calculation using the baseline error detection rate measured in my study. He finds that an outcome changing attack on Georgia's Presidential contest would have resulted in only 832 voters noticing that their BMD ballots showed the wrong selection. Dr. Gilbert suggests that there have not been such complaints from any voters, and says he finds it implausible that so many voters would have "simply not said anything or otherwise simply corrected their ballot and thought nothing of it then or since" (§ 12).

20. This is an oddly constructed hypothetical, since Curling Plaintiffs do not claim here that the Presidential outcome was altered by hacking the BMDs. And Dr. Gilbert does not indicate any effort to determine the total number of spoiled ballots in Georgia's Presidential contest, which he presumably could have explored with State Defendants. Neither does he provide any basis to believe there were only 832 or fewer spoiled ballots. But suppose for the sake of argument that the Presidential election outcome in Georgia had been altered by hacking the BMDs, and there *were* complaints from the 832 voters that Dr. Gilbert has calculated. What then? It seems all but certain that these complaints would have been dismissed or drowned out in the cacophonous aftermath of the election or simply disregarded by election workers at the polling sites as voter errors. Yet the official count, the risk-limiting audit, and the recount would all have found the wrong winner, and there would be no

way to recover any altered vote or correct the election outcome short of rerunning the election. With a mere 832 complaints among 5 million participating voters (amidst a sea of other complaints, real and imagined), it is unlikely that poll workers or election officials, including State Defendants, would realize or even suspected there was a systemic problem with the BMDs, and it is completely implausible that they would take the drastic but necessary step of asking Georgians to vote again. Georgia's election system is susceptible to this extraordinary risk as long as it remains vulnerable to the attacks I described in my report (and potentially others).

21. To get to the point of making a decision to rerun an election, State Defendants (among others, perhaps) would first need to know how many voters discovered a problem when verifying their ballots. As Dr. Gilbert points out, the number of spoiled BMD ballots provides an upper bound on the number of voters who discovered and corrected an error (§ 12). He does not say how many spoiled ballots there actually were in November 2020. If State Defendants knew the number was less than 832, they likely would have shared this fact with Dr. Gilbert, and he would have stated it in his report. It is reasonable to infer that either there were more than 832 spoiled ballots (and the attack is plausible) or State Defendants *do not know* how many BMD ballots were spoiled during the election, eight months later, despite

what Dr. Gilbert acknowledges those ballots would suggest about the reliability of the election.

22. That State Defendants may not know this information is consistent with gaps in other important election data that Georgia counties report to the Secretary of State. State Defendants recently produced electronic data (election projects) that I understand were required to be returned to them by counties after the November 2020 and January 2021 elections. In both elections, a large fraction of counties failed to return any data, returned the wrong data, or omitted data necessary for assessing the security and integrity of the result, such as election databases or ballot images. More than six months after these elections, the Secretary of State has not been able to assemble these electronic records and has not indicated any effort or willingness to do so. Yet the only way that State Defendants could use the number of spoiled ballots as a defense against BMD-based cheating would be if the poll workers accurately tracked it, counties accurately aggregated it, and the Secretary's Office received such data from across the state before the election result was determined. Even then, it is unlikely that the Secretary would be prepared to react by *rerunning the election* if the number of spoiled ballots exceeded the number predicted in an outcome-changing attack.

23. Given the ineffectiveness of such defenses and the critical security problems in Georgia's BMDs, I (like Dr. Appel) recommend that BMDs be reserved for voters who need or request them, as is the case in most states. Dr. Gilbert responds by claiming, without evidence, that "[d]isabled voters are even less likely to identify an error on their printed ballot" (§ 14). I am unaware of any study that supports this sweeping indictment of voters with disabilities, which encompasses a vast array of disabilities that would not impact the ability of the voter to identify an error on their printed ballot in any way. He also contends that blind voters cannot detect errors on their ballot at all, but this is not true. Many blind voters use assistive technology to read printed text and likely could do so to verify their ballots. Moreover, only some voters who need BMDs are blind. For instance, those with motor impairments that prevent them from marking a ballot by hand would not necessarily have any greater difficulty verifying the printed text than any other voter. In any case, if BMDs are used primarily by voters with disabilities (as in most jurisdictions that use BMDs), they will represent a *much* smaller target,⁷ and an

⁷ Although Dr. Gilbert cites a figure that would imply that 10% of Georgians who voted in 2020 were disabled, data from Maryland, where BMDs are available upon request, suggests that only about 1.8% of voters would request to use BMDs if they were offered a hand-marked ballot first. (*Halderman decl.*, Aug. 19, 2020, Dkt. 785-2 at 49.) Dr. Gilbert's citation to the number of all Georgia voters with disabilities is highly misleading since, again, very few of those voters would be

outcome-changing attack on any given election will be detectable with a much lower rate of voter error detection than when all in-person voters use BMDs as they do in Georgia today. This in turn creates a strong disincentive for bad actors to attempt hacking an election (the risk likely is not worth the reward when the outcome is highly unlikely to be changed), which means individual votes would be less likely to be altered by hacking.

24. In his only direct response to my expert report, Dr. Gilbert states that he is not aware that I have “provided equipment marred by ‘undetectable’ hacks to any other independent researcher” (§ 15).⁸ This is a curious and ironic criticism coming from Dr. Gilbert, since he evidently chose not to evaluate my findings through an examination of the voting equipment himself, which he does not explain. Moreover, Dr. Gilbert misreads my report. It does not claim that malicious software infecting a BMD would be undiscoverable by any possible means. If an individual BMD is

unable to vote on a hand-marked paper ballot, consistent with the number reported in Maryland.

⁸ Dr. Gilbert ignores that, as I understand it, State Defendants have objected to my report and the underlying work being shared with third parties (except Dominion), including other independent researchers, with whom I am eager to share my work for review. I am confident in my findings and believe they should be shared promptly with appropriate election security researchers and officials in an effort to mitigate the critical vulnerabilities in Georgia’s voting equipment that I describe. I invite Dr. Gilbert to join me in seeking State Defendants’ consent to do that.

known to contain malware, there will likely be some level of detailed forensic scrutiny that can detect where the malware is, perhaps requiring months of expert analysis per machine at extraordinary expense. It would be completely infeasible to perform this level of analysis on every machine before every election, much less between an election and the deadline for certification of its results. (And after manipulating ballots, malware could remove all traces of its presence from a machine, defeating any possible post-election examination of the device.) What my report shows is that vote-stealing malware of the type I have constructed would not be detected by any of the defenses that State Defendants purport to practice. I describe in detail how such malware would defeat QR code authentication, logic and accuracy testing, on-screen hash validation, and external APK validation (as was used by Pro V&V after the November election). Dr. Gilbert offers no rebuttal to these findings. He does not dispute them or even address them.

25. Moreover, there is already an example of an “undetectable” attack entered into testimony: exploitation of the Drupal vulnerability discovered by Logan Lamb in the Center for Election Systems server. As Lamb attested, the developers of the primary tool for detecting this vulnerability stated that “[n]either [the defensive tool] nor an expert can guarantee a website has *not* been compromised. They can only

confirm with certainty a website *has* been compromised.”⁹ Furthermore, the Drupal developers state that any server running the vulnerable software after the initial disclosure of the vulnerability should be assumed to have been compromised unless it was patched within *hours* of disclosure. According to the timeline presented in Lamb’s declaration, he found the KSU server to be in a vulnerable state on August 28, 2016, nearly two years after the initial announcement of the critical vulnerability (October 15, 2014).¹⁰ The KSU server image also contains evidence that a second vulnerability, the so-called Shellshock flaw, was exploited on December 2, 2014.¹¹ This vulnerability was publicly disclosed more than two months earlier and widely publicized in the media as a critical vulnerability, yet the KSU server remained unpatched.

26. An attacker who compromised the KSU server could therefore have maintained undetected access to the compromised server. Since the server remained in a vulnerable state undetected for almost two years, it is highly likely that it was successfully attacked at some point in time. An attacker who did so would have been able to move laterally to other systems within the CES network and to other

⁹ *Lamb decl.*, Dkt. 258-1 at 19.

¹⁰ See “Drupal Core - Highly Critical - Public Service announcement” (Oct. 29, 2014), available at <https://www.drupal.org/PSA-2014-003>.

¹¹ *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 23.

components of Georgia's voting system. As I have previously pointed out, many election system components that could have been compromised in this way are still in use in Georgia today, where they provide a means by which attackers could spread vote-stealing malware to the BMDs.

27. Rather than address the many threats to Georgia's voting system, Dr. Gilbert persists in drawing illogical comparisons between BMDs and hand-marked paper ballots. For instance, he questions why Plaintiffs have presented no research "regarding voters' proclivity to review [hand-marked paper ballots] to ensure their ballots are marked and will count as intended" (§ 8). Much like Dr. Gilbert's earlier testimony that "[i]n essence, a BMD is nothing more than an ink pen,"¹² one does not need expertise in election security to find fault with this reasoning. Preventing voters from making accidental mistakes is a completely different problem from preventing their selections from being deliberately and systematically changed by an attacker who has compromised the BMDs. There is abundant evidence that voters do sometimes make errors whether filling out a ballot by hand or by machine. Bad ballot design exacerbates this problem with both voting modalities, but following ballot design best practices can greatly reduce it. Both

¹² *Gilbert decl.*, Dkt. No. 658-3 at 60.

BMDs and scanners that count hand-marked ballots can also be configured to reject overvotes and to warn voters about undervotes, the most common kinds of voter errors. Moreover, unlike older technologies for counting hand-marked ballots, the scanners used in Georgia (when properly configured) can detect improperly or incompletely marked bubbles and present them to human operators to adjudicate whether the marks should count as votes. Election officials can use all of these options to help protect voters from their own mistakes, but none of them offers protection against a BMD that deliberately changes the selections printed on a voter's ballot (or those encoded in the ballot barcode). The central problem with Georgia's highly vulnerable BMD system—that attackers can change all records of the voter's intent without being detected by election officials—has no parallel in a hand-marked paper ballot system.

28. Dr. Gilbert concludes as he started, with vague and sweeping generalities. “Simply put, BMD elections systems are no more insecure than [hand-marked] systems” (¶ 16). It is unclear whether he is claiming that *all* BMD systems are at least as secure as all hand-marked systems or merely that some specific BMD system (such as the one he recently developed himself to address some of the reliability problems that exist with Georgia's BMDs) is at least as secure as some hand-marked system, but this is of little consequence. The only BMD system that is

relevant here is the Dominion ICX as used in Georgia. As my expert report details, Georgia's BMD system suffers from numerous, severe vulnerabilities. These vulnerabilities would have little potential to change election outcomes if use of BMDs were limited to voters who need or request them, as Curling Plaintiffs desire, and they would be far less likely to affect the personal votes of individual Georgia voters.

Reply to Declarations of Dr. Benjamin Adida

29. The declarations by Dr. Adida that State Defendants have submitted predate my expert report, so Dr. Adida's opinions are not informed by the critical vulnerabilities in Georgia's BMD equipment that my analysis has revealed or by anything else in my lengthy, detailed report. Nor are they informed by any events that occurred in the year since he first provided these declarations, such as any aspect of the November 2020 election in Georgia or the Secretary of State's study indicating that few voters verified their respective ballots in that election.

30. Nevertheless, Dr. Adida's first declaration is correct that "Running a risk-limiting audit is one of the most important advances states can take in improving election integrity—without an RLA, we are effectively trusting computerized scanners to count our paper ballots" (Dkt. 834-2 at ¶ 5). This is true, but, as my expert report shows, without a risk-limiting audit Georgia is also trusting its critically

vulnerable BMDs to generate ballots with QR codes that correctly reflect voters' selections. Obviously compromised BMDs and compromised scanners could change individual votes and election outcomes. But again, nothing suggests that Georgia's scanners suffer from such easily exploitable critical vulnerabilities as the BMDs do.

31. Dr. Adida and I also agree that RLAs are important for discovering whether compromised BMDs have manipulated enough ballot QR codes to change the outcome of an election (§ 12). Although RLAs are, as Dr. Adida says, "of the utmost importance" (§ 6), Georgia does not require an RLA in the vast majority of elections and the vast majority of contests, leaving both election outcomes and individual voters' votes susceptible to manipulation via BMD malware. Additionally, it is insufficient for states to merely (in Dr. Adida's words) "take meaningful steps to implement RLAs"; rather, states have to *actually conduct* reliable RLAs, which Georgia does not intend to do for the vast majority of its elections (or perhaps any of its elections, depending on the reliability of the audit procedures it implements).

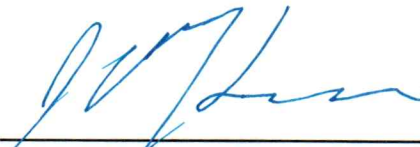
32. In his second declaration, Dr. Adida refers to a "dispute amongst academics regarding whether voters verify their ballots using ballot-marking devices" (Dkt. 912-1 at § 11). This statement reflects a misunderstanding of the state of research today. I am not aware of any scientific research that supports the proposition that Georgia voters would likely detect more than a small fraction of

errors caused by BMD malware. In contrast, the past two years have seen a wave of laboratory studies and multiple field observation studies addressing this question, all of which strongly indicate the opposite, that few voters carefully review their ballots and so the vast majority of errors caused by BMD malware would likely to go undiscovered and uncorrected. Although there once was uncertainty about whether most voters carefully verify their BMD ballots, there is no longer any serious scientific dispute that they do not. It is the hallmark of good science (and of good public policy) that it evolves based on new evidence, such as the University of Georgia study commissioned by the Secretary of State that I discussed above—which Dr. Adida has not addressed.

33. Georgia's election system needs to evolve as well. Due to the critical vulnerabilities in Georgia's BMDs that are described in my expert report, Georgia voters face an extreme risk that BMD-based attacks could manipulate their individual votes and alter election outcomes. Even in the rare contests for which the State requires a risk-limiting audit, the scientific evidence about voter verification shows that attackers who compromise the BMDs could likely change individual votes and even the winner of a close race without detection. Georgia can eliminate or greatly mitigate these risks by adopting the same approach to voting that is practiced in most of the country: using hand-marked paper ballots and reserving

BMDs for voters who need or request them. Absent security improvements such as this, it is my opinion that Georgia's voting system does not satisfy accepted security standards. Neither Dr. Gilbert nor Dr. Adida offers a contrary opinion in their respective declarations, instead ignoring the critical issue of whether the *voting system used in Georgia*—which neither claims to have examined—reliably protects the right to vote for individual Georgia voters.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 2nd day of August, 2021 in Rushland, Pennsylvania.



J. ALEX HALDERMAN

CYBERSECURITY

Georgia election systems could have been hacked before 2016 vote



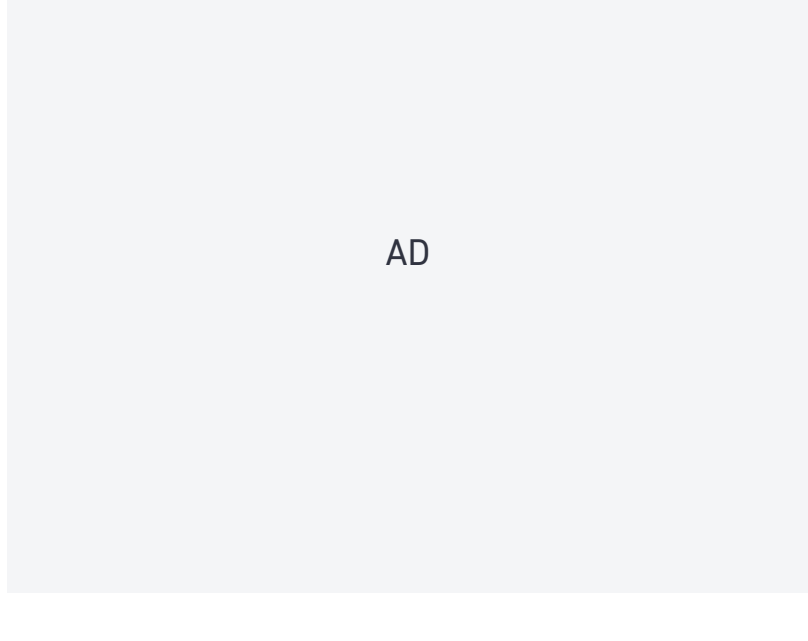
Georgia has been at the center of questions about voter security, due to the fact the state has used insecure paperless voting machines since 2002. | David Goldman/AP Photo

By KIM ZETTER
01/16/2020 11:07 PM EST



A Georgia election server contains evidence that it was possibly hacked before the 2016 presidential election and the 2018 vote that gave Georgia Gov. Brian Kemp a narrow victory over Democratic opponent Stacey Abrams, according to an election security expert.

The incident, which occurred in late 2014, long before either of those elections, not only calls into question the integrity of Georgia's voting machines during critical elections, but raises new questions about whether attackers were able to manipulate election data and voter information through the compromised server.



It's unclear who may have carried out the alleged attack or if voter information was altered, but Logan Lamb, the election security expert who uncovered the activity, believes that if hackers did breach the server, they could have gained “almost total control of the server, including abilities to modify files, delete data, and install malware.”

Georgia has already been at the center of questions about voter security, due to the fact that the state has used insecure paperless voting machines since 2002.

Additionally, Georgia counties were among those that Russian hackers targeted in 2016 when they breached some state websites and probed others for vulnerabilities that would have given them access to voter registration databases and other election data and systems.

The Georgia server in question has been at the heart of a 2018 lawsuit brought by election integrity activists seeking to bar Georgia from using its paperless voting machines.

Lamb, who is an expert witness for the plaintiffs, uncovered the anomalies in an investigation for the plaintiffs. The allegation about the server, first reported by The Associated Press, were contained in an affidavit from Lamb filed Thursday in Atlanta federal court as part of the lawsuit.

Lamb declined to speak with POLITICO due to a court order, but one of the groups behind the case said his findings paint a disturbing picture about the state of elections in Georgia.

“It creates a very dark cloud over all of the previous elections because as we know there was no way to audit them, there was no ... attempt at accountability by the secretary of state, and the entire programming of elections was outsourced,” said Marilyn Marks, executive director of the Coalition for Good Governance, one of the groups behind the lawsuit.

“[W]hat Logan’s findings show us ... is that vulnerabilities were not just hypothetical as the state had been claiming. Now we know that it was a very real risk, but what we don’t know is just how bad did it get. And the public deserves to know,” she said.

Georgia used the server to distribute critical election and voter registration files to counties throughout the state. The state has insisted, however, that it never distributed files to program voting machines through the server. Instead, it delivered these files to counties physically. But if the server was compromised, it could have been a vehicle to distribute malware to any county election worker who connected to it.

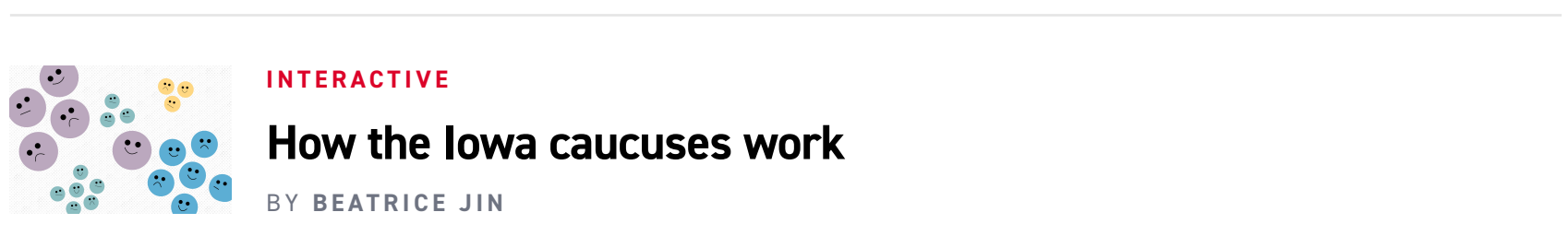
Georgia’s secretary of state, Brad Raffensperger, did not respond immediately to a request for comment. Kemp served as secretary of state at the time of the 2016 election, before being elected governor in 2018.

The Center for Election Systems at Kennesaw State University, which was responsible for programming all of the voting machines in Georgia before every election, owned and operated the server in question. That server was already known to have security issues.

As POLITICO first reported, months before the 2016 election, Lamb discovered that the KSU server was improperly secured so that anyone could access sensitive election data stored on it, and it also had an unpatched vulnerability in so-called Drupal software the server used, which would have allowed attackers to take control of the server and alter or delete data on it, or to post malware that could have infected the computers of election officials accessing the server.

Logan made the discovery by chance when he visited the Center for Election Systems website to learn more about their role in programming voting machines for Georgia.

After the POLITICO story published in June 2017, the plaintiffs filed their lawsuit and sought to obtain the server for evidence supporting their contention that Georgia’s election systems are not secure and could have been tampered with in the 2016 election.



But officials at Kennesaw wiped the server clean shortly after the plaintiffs filed their suit. The FBI had a mirror image of the server, which had been made in March 2017, but state officials fought to prevent the plaintiffs from obtaining it to examine. They lost that fight last year.

Only recently was Lamb able to examine the server for evidence of tampering. In his affidavit, Lamb said the server appears to have been compromised in December 2014, using an unpatched vulnerability called “Shellshock” that had been publicly revealed and widely reported three months earlier.

The Shellshock vulnerability is different from the Drupal one Lamb discovered when he visited the Center’s website in 2016. Both the Shellshock and Drupal vulnerabilities had been publicly exposed around the same time, but despite both receiving extensive media coverage and even a Department of Homeland Security alert in the case of Shellshock, officials at the Center for Election Systems failed to apply a patch to close either of them when the patches were released.

Although a log on the server shows some of the alleged intruder’s activity on it, there are signs the intruder may have deleted important information from the log, preventing Lamb from viewing everything that occurred.

A different log on the server that recorded access to the server’s content-management system — the software the Center used to publish files and content on the Center’s website for election officials to access — also thwarted Lamb’s investigation because he had access to records going back to only Nov. 10, 2016, a few days after the 2016 election. This prevented him from seeing who might have accessed the content-management system prior to that date or altered its contents.

Lamb suggests in his court document that the logs were deleted intentionally and this was done for suspicious reasons.

“I can think of no legitimate reason why records from that critical period of time should have been deleted,” he wrote.

But it’s not uncommon for log files to record data for only a certain time period before they overwrite those records. Information about Drupal’s access log published on a forum for Drupal developers and users indicates its access log saves data for only 16 weeks before deleting and overwriting it.

The other log Lamb was able to examine for the server itself does go back further, and this log shows that on Dec. 2, 2014, a new user named “Shellshock” was created on the server — the same name as the widely known vulnerability that was apparently used to get into the server.

About 15 minutes later, the log shows, the Shellshock vulnerability was patched on the server.

It’s common for hackers to immediately patch the vulnerability they used to access a system, in order to keep other potential attackers out and maintain their control of the system. Although it could have been a system administrator who patched the server and created the Shellshock user account, a security expert told POLITICO it’s unlikely.

“If I were a [system administrator], why would I create it and call it the same name as the [vulnerability]?” said Kevin Skoglund, an independent security expert. He said the suspicious name of the user account suggests the attackers may have been using automated software to scan for internet-connected servers containing the flaw. Once their malicious software found a vulnerable system, it may have been programmed to then automatically create a Shellshock user account on the system.

Lamb wrote in the court document that evidence in the log made it appear that the Shellshock user also tried to hide their activity once on the server. The log records a history of any commands initiated on the server, but it contained only a couple commands, suggesting the intruder may have deleted others.

There could be reasonable explanations for the suspicious activity Lamb spotted on the server.

“There may still be other explanations. It is possible, for example, that a CES employee” was the person behind the unusually named Shellshock account, he wrote in his court document.

But if a CES worker did apply the Shellshock patch in December, following the extensive media covered the Shellshock vulnerability had received three months earlier in September, it’s odd that they didn’t also patch the Drupal vulnerability that was publicly disclosed in October that year. The latter vulnerability was still on the server in August 2016 when Lamb visited it.

He believes the evidence points to an intruder.

“The long unpatched software, unusual username, potentially modified command history, and near immediate patching of the Shellshock bug are all strong pieces of evidence that an outside attacker gained access to the KSU server by exploiting the Shellshock bug,” he wrote. Further investigation would need to be done to confirm this, he noted.

FILED UNDER: CYBER SECURITY, GEORGIA, ELECTION CYBERSECURITY

Huddle

A play-by-play preview of the day's congressional news

EMAIL

Your Email

INDUSTRY

Select Industry

EMPLOYER

Employer

All fields must be completed to subscribe.

By signing up you agree to allow POLITICO to collect your user information and use it to better recommend content to you, send you email newsletters or updates from POLITICO, and share insights based on aggregated user information. You further agree to our [privacy policy](#) and [terms of service](#). You can unsubscribe at any time and can [contact us here](#). This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

SIGN UP

About Us | Advertising | Breaking News Alerts | Careers | Credit Card Payments | Digital Edition | FAQ | Feedback | Headlines | Photos | POWERJobs | Press | Print Subscriptions | Write For Us | RSS | Site Map

Terms of Service | Privacy Policy | Do not sell my info | Notice to California Residents

© 2022 POLITICO LLC

Case 1:21-cv-00317-DCLG-CHS Document 67-4 Filed 03/17/22 Page 1 of 1 PageID #: 2577