**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MINNESOTA**

SMARTMATIC USA CORP.,
SMARTMATIC INTERNATIONAL
HOLDING B.V., and SGO
CORPORATION LIMITED,

Plaintiffs,

v.

MICHAEL J. LINDELL and MY
PILLOW, INC.,

Defendants.

Case No. 22-cv-0098-WMW-JFD

# **<u>MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTION TO COMPEL</u>**

## TABLE OF CONTENTS

INTRODUCTION .......... 1

FACTUAL BACKGROUND .......... 3

I. LA County Implemented Its VSAP Initiative To Improve The Voting Experience For Its Residents And Improve Election Security .......... 3

II. Smartmatic Contracted With LA County To Provide BMDs And Related Source Code. .......... 4

III. The Source Code Developed By Smartmatic Was Certified After A Rigorous Testing Process. .......... 5

IV. The Source Code And Trusted Build Files Were Placed In A Highly Secure Escrow Account After Certification. .......... 7

V. MyPillow Served Requests For Production Of Smartmatic's BMDs And Source Code. .......... 9

LEGAL STANDARD .......... 10

ARGUMENT .......... 11

I. Smartmatic Does Not Have Possession, Custody, or Control Of The Requested Materials. .......... 12

A. Smartmatic Does Not Have Actual Possession Of LA County's BMDs And Source Code. .......... 12

B. Smartmatic Does Not Have The Legal Right To Obtain The BMDs and Source Code Requested By MyPillow .......... 15

II. The Court Should Deny Defendants' Motion Because Defendants' Requested Inspection Is Not Necessary. .......... 17

A. Courts Reject Requests To Inspect Highly Confidential Source Code When The Inspection Is Not Necessary .......... 17

B. Defendants' Requested Inspection Of Highly Confidential Voting Technology Is Not Necessary. .......... 19

1. Disclosure Of The Requested Materials Would Threaten Election Security. .......... 20

2. Other Sources Of Information Adequately Address The Issues That Defendants Seek To Probe. .................................... 24

CONCLUSION ........................................................................................................ 29

# TABLE OF AUTHORITIES

**Page(s)**

**Cases**

*Beyond Blond Prods., LLC v. Hall*,
No. 22-MC-0037 (JFD), 2022 WL 3444039 (D. Minn. Aug. 17, 2022) ..................... 11

*Blue Spike, LLC v. Vizio, Inc.*,
No. 8:17-cv-01172-DOC-KESx, 2018 WL 8646476 (C.D. Cal. July 3, 2018) ..................... 15

*Congoo, LLC v. Revcontent LLC*,
No. 16-401 (MAS), 2017 WL 3584205 (D.N.J. Aug. 10, 2017) ..................... *passim*

*Cook Cty. Republican Party v. Pritzker*,
487 F. Supp. 3d 705 (N.D. Ill. 2020) ..................... 20

*Edeh v. Equifax Info. Servs., LLC*,
291 F.R.D. 330 (D. Minn. 2013) ..................... 12

*Elsherif v. Mayo Clinic*,
No. 18-cv-2998-DWF-KMM, 2020 WL 5015825 (D. Minn. Aug. 25, 2020) ..................... 11

*Lindell v. United States*,
No. 0:22-cv-2290 (D. Minn. 2022) ..................... 23

*List v. Carwell*,
No. 18-cv-2253, 2020 WL 5988514 (D. Minn. Oct. 9, 2020) ..................... 12, 15, 17

*Neo Ivy Capital Mgmt. LLC v. Savvysherpa LLC*,
No. 18-mc-0094, 2019 WL 1435058 (D. Minn. Mar. 8, 2019) ..................... 18

*Northbrook Digital, LLC v. Vendio Servs.*,
625 F. Supp. 2d 728 (D. Minn. 2008) ..................... 24

*Nutratech, Inc. v. Syntech Int'l, Inc.*,
242 F.R.D. 552 (C.D. Cal. 2007) ..................... 24

*Peterson v. Seagate U.S. LLC*,
No. 07-2502, 2009 WL 3430150 (D. Minn. Oct. 19, 2009) ..................... 18, 24, 28

*Prokosch v. Catalina Lighting, Inc.*,
193 F.R.D. 633 (D. Minn. 2000) ..................... 12

*Purcell v. Gonzalez*,
549 U.S. 1 (2006) ... 20

*Roark v. Credit One Bank, N.A.*,
No. 16-173, 2016 WL 11606777 (D. Minn. Dec. 1, 2016) ... 16

*Saleh v. Nike, Inc.*,
No. CV 20-09581-FLA (RAOx), 2021 WL 4434352, at *2 (C.D. Cal. Aug. 16, 2021) ... 18, 19, 24, 28

*Viacom Int'l Inc. v. YouTube Inc.*,
253 F.R.D. 256 (S.D.N.Y. 2008) ... 18, 20, 21, 24

**Other Authorities**

*California*, American Presidents Since 1960, *available at* https://www.americanpresidents.net/states/california.php (last accessed on Feb. 15, 2023) ... 1

*Election Infrastructure Security*, Cybersecurity & Infrastructure Security Agency, *available at* https://www.cisa.gov/election-security (last visited Feb. 15, 2023) ... 20

*Election Security*, Department of Homeland Security, *available at* https://www.dhs.gov/topics/election-security (last visited Feb. 15, 2023) ... 20

Fed. R. Civ. P. 26(b)(1) ... 10, 18

Fed. R. Civ. P. 26(b)(2)(C) ... 18

Fed. R. Civ. P. 34 ... 12

Fed. R. Civ. P. 34(a) ... 12

*Jimmy Kimmel Live* (ABC television broadcast Jan. 31, 2023), *available at* https://www.youtube.com/watch?v=vGlDEbZvwLI. (last visited Feb. 15, 2023) ... 23

Natalie Musumeci, Warren Rojas, & Cheryl Teh, *Supreme Court won't let MyPillow CEO Mike Lindell dodge Dominion's $1.3 billion defamation lawsuit* (Oct. 3, 2022), https://www.businessinsider.com/supreme-court-rejects-mike-lindell-mypillow-dominion-lawsuit-2022-10 (last visited Feb. 15, 2023) ... 23

Olivia Rubin & Soo Rin Kim, *Voting machine company sues pro-Trump pillow man over false election claims*, ABC NEWS (Feb. 22, 2021, 11:07 AM), https://abcnews.go.com/US/voting-machine-company-sues-pro-trump-pillow-man/story?id=76043949 (last visited Feb. 15, 2023) ............................ 22

Asawin Suebsaeng, Lachlan Cartwright, & Adam Rawnsley, *Dominion Says It Will Sue MyPillow CEO Mike Lindell Over Election Fraud Claims*, The Daily Beast (Feb. 16, 2021), https://www.thedailybeast.com/dominion-says-it-will-sue-mypillow-ceo-mike-lindell-over-election-fraud-claims (last visited Feb. 15, 2023) ................... 22

## INTRODUCTION

In their two-year disinformation campaign and in discovery, Defendants Michael J. Lindell and My Pillow, Inc. ("MyPillow") have failed to disclose a shred of evidence that, as they claim, Smartmatic "rigged" the 2020 U.S. Presidential Election ("2020 Election"). Nor could any such evidence exist because, as every credible source of information has recognized, neither Smartmatic nor any other voting technology company tampered with the vote count in the election. Nevertheless, in an effort to sell more pillows to individuals disappointed in the outcome of the election, Defendants continue to publish the lie that Smartmatic "flipped" votes from Donald Trump to Joe Biden. They also tell their supporters that they will use discovery in this case to finally uncover the smoking gun that the election was rigged and expose the "truth" to the world.

To that end, Defendants have moved to compel the production of voting technology that Smartmatic provided to Los Angeles County ("LA County") for use in the 2020 Election. LA County is the only jurisdiction that contracted with Smartmatic for purposes related to the 2020 Election and California was not even a battleground state.[1] These facts, alone, preclude the possibility that Smartmatic rigged the election. Defendants nevertheless claim that they need to inspect the hardware and source code that Smartmatic provided to LA County to test their conspiracy theories.

[1] A Republican candidate has not carried the State of California in a U.S. Presidential election since 1988. *Presidential Voting History of California*, AMERICAN PRESIDENTS SINCE 1960, *available at* https://www.americanpresidents.net/states/california.php (last accessed on Feb. 15, 2023).

The Court should deny Defendants' motion for multiple reasons. As a threshold matter, Smartmatic does not possess the requested materials. Defendants have requested an exemplar of the Smartmatic ballot marking device ("BMD") used in the 2020 Election and the source code that was used in the election. Smartmatic's BMDs could not have rigged the election because they merely print paper ballots that a voter can verify after making their selections, and they do not tabulate votes. Regardless, Smartmatic does not possess BMDs used in the election—they are exclusively owned by LA County and maintained on LA County property. Nor does Smartmatic possess the executable code that LA County installed in the BMDs for the election. The code installed in the BMDs is owned by LA County, and as required by law, it is stored in an escrow account that Smartmatic could not access prior to the election and cannot access now.

The Court should also deny Defendants' motion because they have not established that they need to inspect highly confidential election technology. Indeed, alternative sources—including reports published by the California Secretary of State—preclude any need for the inspection. These sources address the topics that Defendants claim they need to explore, including whether Smartmatic could have "flipped" votes from Donald Trump to Joe Biden. Reliance on alternative sources is particularly appropriate because Lindell is a threat to publicly disclose any materials he obtains. During his crusade to "melt the machines and turn them in to prison bars," he has stated that he intends to use discovery to serve his own agenda, and the FBI has even executed a search warrant on him related to potential crimes for unlawfully accessing voting technology. In short, Defendants cannot be trusted with LA County's highly confidential voting technology.

## FACTUAL BACKGROUND

### I. LA County Implemented Its VSAP Initiative To Improve The Voting Experience For Its Residents And Improve Election Security.

The Registrar-Recorder/County Clerk of the County of Los Angeles operates one of the most extensive and complex voting operations in the United States to serve a diverse population larger than that of most states. (Declaration of James Long ("Long Decl.") ¶ 3.) After finding commercially available options insufficient to meet the County's needs and to address the compelling needs for secure elections, verified results, and universal voter access, the Registrar-Recorder/County Clerk directed development of its Voting Solutions for All People (VSAP) voting system. (*Id.*) The VSAP initiative sought to ensure that voters in Los Angeles County had greater opportunities to participate by providing expanded options for voting in a manner that is convenient, accessible, and secure. (*Id.*)

The VSAP Voting System includes a number of components, including: (i) a Redesigned Vote-by-Mail ("VBM") Ballot for voters who wish to vote by mail; (ii) an Electronic Pollbook ("e-Pollbook") to check-in voters at poll stations; (iii) an Interactive Sample Ballot ("ISB") that voters can use before arriving at poll stations to expedite the voting process; and (iv) a Tally System, which is VSAP's innovative solution for paper ballot scanning and tabulation. (*Id.* ¶ 4.) In addition to the components described above, the VSAP Voting System includes a ballot marking device ("BMD"). (*Id.* ¶ 5.) The BMD is the primary voter interface system and consists of a touchscreen, an audio and tactile controller, and dual-switch input that voters use to generate, verify, and cast a paper ballot. (*Id.*) The BMD allows every voter to customize their experience with both visual and audio access in numerous languages and offers accessibility features that provide voters with disabilities equality, privacy, and independence in casting ballots. (*Id.*)

For auditability and security, the BMD prints human-readable paper ballots. (*Id.* ¶ 6.) After verifying that the printed ballot is correct, the voter then inserts the completed ballot back into the BMD, which transfers the ballot to the Integrated Ballot Box, attached to the BMD. (*Id.*) The completed ballots are later collected and tallied using the Tally System. (*Id.*) The BMD is not connected to the internet. (*Id.* ¶ 7.) Nor does the BMD retain voting results or tabulate or count votes. (*Id.*)

## II. Smartmatic Contracted With LA County To Provide BMDs And Related Source Code.

In June 2018, Smartmatic entered into a contract with LA County to continue previous work on the development, manufacturing, and implementation of BMDs as part of the VSAP initiative. (Long Decl. ¶ 8.) Smartmatic provided the following technology and services to LA County: (1) engineered and manufactured the BMD hardware, (2) programmed the BMD software, (3) facilitated the California certification process, (4) created the backend software to manage the devices, (5) provided systems integration services, (6) managed the build-out of the VSAP operations center, (7) handled logistics and setup/breakdown of the vote centers, (8) oversaw real-time data management for deployment, and (9) supplied Help Desk services on Election Day. (*Id.*) Smartmatic did not have any role in the development or manufacturing of the e-Pollbook or the Tally System used to tabulate the paper ballots. (*Id.*)

Under the contract between the parties, LA County retains full ownership of intellectual property rights to the software developed by Smartmatic, as well as ownership of the BMDs themselves. (*Id.* ¶ 9; *see also* Declaration of Michael E. Bloom ("Bloom Decl.") ¶ 3, Ex. 1, LA County Contract §§ 2.1.1, 2.3.1 (granting LA County ownership over all materials and intellectual property related to the VSAP technology produced by Smartmatic).) Smartmatic performs maintenance as needed on BMDs in service. (Long Decl. ¶ 26.) The BMDs are stored at a facility owned by LA County and Smartmatic performs maintenance on them at the LA County facility. (*Id.*)

## III. The Source Code Developed By Smartmatic Was Certified After A Rigorous Testing Process.

Since its initial deployment in 2018, the California Secretary of State ("SOS") has certified five versions of the VSAP Voting System: 1.0, 2.0, 2.1, 2.2, and 3.0. (Long Decl. ¶ 11.) VSAP Voting System 2.2 was utilized by LA County in the U.S. Presidential General Election on November 3, 2020. (*Id.*) Smartmatic was responsible for developing the BMD software for VSAP Voting Systems 2.0, 2.1, 2.2, and 3.0. (*Id.* ¶ 12.)

Once development of the voting system was finalized, LA County submitted an application for approval of a voting technology to the California SOS. (*Id.* ¶ 13.) Pursuant to the California Elections Code ("CEC"), prior to considering any new voting technology for approval, or any modification to a currently approved voting technology, the California SOS must conduct an examination of the proposed system. (*Id.*) The examination and testing of the VSAP Voting System included the examination of application and technical documentation; development of a detailed system test plan that reflects the scope and complexity of the system; code review for software components; a trusted build to conclusively establish the system version and components being tested; operation and function testing of hardware and software components; security testing that includes a full source code review and penetration testing; volume testing of the system and/or all devices with which the end user directly interacts; functional and performance testing of the integrated system, including testing of the full scope of system functionality, and performance tests for telecommunications and security; examination and testing of the system operations and maintenance manual; and accessibility examination and testing. (*Id.* ¶ 14.)

This extensive testing was conducted by an accredited independent testing authority. (*Id.* ¶ 15.) For VSAP Voting Systems 2.1 and 2.2, the independent testing authority was SLI Compliance. (*Id.*) SLI Compliance is accredited by the Election Assistance Commission for voting system testing. (*Id.*) SLI Compliance issued a number of reports in connection with its testing of VSAP Voting System 2.1. (*See, e.g.,* Bloom Decl. ¶¶ 4-5, Ex. 2-3.)

After testing was completed, and the software source code finalized, the independent testing authority oversaw what is known as the "trusted build." (Long Decl. ¶ 16.) Software is written by programmers in a human-readable programming language. (*Id.*) This human-readable code is referred to as the source code. (*Id.*) During the trusted build process, the source code was transformed into a format that can be executed by a computer, known as machine code or assembly code. (*Id.*) This executable program, built utilizing the software source code, is the trusted build. (*Id.*)

Upon completion of the trusted build, the independent testing authority created an immutable hash value that uniquely identifies the code built. (*Id.* ¶ 17.) A hash is a mathematical function that creates a unique string of letters and numbers that identifies a system and its programming. (*Id.*) After creation of the hash value for a software file, any modification to the file will result in that file returning a different hash code, allowing vendors and elections officials to compare hash values and confirm that the voting system and its source code has not been altered. (*Id.*)

The independent testing authority then provided the trusted build file to LA County. (*Id.* ¶ 18.) VSAP Voting System 2.1 was approved by the California SOS on October 1, 2020. (*Id.* ¶ 19; *see also* Bloom Decl. ¶ 6, Ex. 4, VSAP 2.1 Conditional Approval.) On October 6, 2020, the SOS issued an administrative approval of VSAP Voting System 2.2, which made minor modifications to VSAP 2.1. (Long Decl. ¶ 19; *see also* Bloom Decl. ¶ 7, Ex. 5, VSAP 2.2 Administrative Approval.)

## IV. The Source Code And Trusted Build Files Were Placed In A Highly Secure Escrow Account After Certification.

Within ten business days of approval by the California SOS, LA County was required by the CEC to deposit the trusted build files, along with the software source code, to a State of California approved escrow facility. (Long Decl. ¶ 20.) As required by law, access to the materials in escrow is extremely limited. (*Id.*) Smartmatic was not involved in conveying the trusted build and source code files to the escrow facility and did not (and does not) have access to the files placed in escrow. (*Id.* ¶ 21.)

In preparation for the 2020 Election, LA County accessed the trusted build files contained in the escrow account. (*Id.* ¶ 22.) Using the hash code, the County independently confirmed that the trusted build files received from the escrow account were identical to those that were reviewed and tested by the independent testing authority. (*Id.*) LA County then installed those trusted build software files onto the voting system hardware. (*Id.* ¶ 23.) Smartmatic had no access to the trusted build files during this process. (*Id.*)

As an additional security mechanism, the VSAP Voting System incorporated an Electronic Signing Authority ("ESA"). (*Id.* ¶ 24.) The ESA is a method of encryption used to ensure each component of the VSAP system is conforming to security standards and to help ensure that the data being passed to components are secure and authenticated. (*Id.*) This system utilizes a pair of encryption keys that allow the voting system hardware to confirm that the software loaded onto the hardware is the verified trusted build file. (*Id.*) Utilizing these encryption keys, if the software loaded onto the hardware is not identical to the trusted build file, the software will crash and the machine will not be usable. (*Id.*) LA County is in sole possession of the encryption keys; Smartmatic has never had access to the encryption keys. (*Id.*)

In its capacity as an LA County contractor, and subject to the permission of LA County and restrictions implemented by LA County, Smartmatic has access to a database containing the copy of the source code that it provided to the independent testing authority on LA County's behalf and the trusted build file that the independent testing authority subsequently created. (*Id.* ¶ 25.) But Smartmatic does not have access to the trusted build or software source code files stored in the escrow account, including the trusted build file withdrawn from the escrow account by LA County and installed by it in the BMDs used in the 2020 Election. (*Id.*)

## V. MyPillow Served Requests For Production Of Smartmatic's BMDs And Source Code.

On November 4, 2022, MyPillow served its First Set of Requests for Production of Documents and Things to Smartmatic. (ECF No. 76-1, Ex. A.) It requested, in pertinent part:

- An exemplar of each Smartmatic Product used by any county, precinct, election site, or polling location in the State of California to administer the 2020 Presidential Election (Request No. 1);
- The source code for any Smartmatic Product, Hardware, Software, or systems used in the 2020 Presidential Election in any county, precinct, election site, or polling location in the State of California (Request No. 8); and
- Any Hardware and Software in the possession, custody, or control of Smartmatic that was used to administer the 2020 Presidential Election in any jurisdiction in any State (Request No. 10).

(*Id.* at Request Nos. 1, 8, 10.)

On December 5, 2022, Smartmatic served its responses to MyPillow's requests. (ECF No. 76-1, Ex. B.) Smartmatic generally objected to MyPillow's requests to the extent that they "seek disclosure of information that is not in Smartmatic's possession, custody, or control." (*Id.* at 4.) It also specifically objected to Request Nos. 1, 8, and 10, on several grounds, including that the requests seek information or documentation protected from disclosure under confidentiality or other agreements with third parties.

(*Id.* at 6, 10-12.) Nevertheless, in response to RFP No. 1, Smartmatic agreed to produce user manuals and guides relating to the VSAP components developed by Smartmatic for use in the 2020 Election, to the extent they exist and can be located by a reasonable search. (*Id.* at 6.)

On February 7, 2023, Defendants sent Smartmatic notices of subpoenas that they intend to serve on LA County and the California SOS. (Bloom Decl. ¶¶ 8-9, Ex. 6-7.) Defendants included a list of "Items To Produce" in their subpoenas. (*Id.*) The requested items include all sorts of documents and information related to VSAP and Smartmatic's work for LA County in connection with the 2020 Election. (*See id.*) Most pertinently, Defendants intend to seek from the California SOS "[a] forensic copy of each version of ballot marking system source, voting system source code, or other code created, licensed, or sold by Smartmatic which was used in the 2020 General Election." (*Id.* ¶ 9, Ex. 7 at 4.) They also intend to request that LA County produce "[d]ocuments related to [LA County's] deposit of an exact copy of the trusted build files to the State of California approved escrow facility," and "[a] forensic copy of each non-identical copy of the source code, application control system, BMD internal system, cast vote record, or any other software by [sic] Smartmatic to You for use in any ballot marking device . . . that was used to administer the 2020 General election." (*Id.* ¶ 8, Ex. 6 at 4-5.)

## LEGAL STANDARD

The Federal Rules of Civil Procedure permit liberal discovery regarding "any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1). Discovery is not, however, unlimited.

*Elsherif v. Mayo Clinic*, No. 18-cv-2998-DWF-KMM, 2020 WL 5015825, at *2 (D. Minn. Aug. 25, 2020). "Discovery that is unreasonably burdensome, cumulative, or outside of the scope permitted by 26(b)(1) should be limited by the Court." *Id.*

"The party that seeks discovery has the burden of making a threshold showing that the information sought is relevant to the claims or defenses in the case." *Beyond Blond Prods., LLC v. Hall*, No. 22-MC-0037 (JFD), 2022 WL 3444039, at *2 (D. Minn. Aug. 17, 2022) (Docherty, J.) (citation omitted). Then, "the party resisting production bears the burden of establishing lack of relevancy or undue burden." *Id.* (citation omitted).

## ARGUMENT

The Court does not need to reach the issue of whether Defendants can properly inspect LA County's BMDs and source code because Smartmatic does not have possession, custody, or control of them. Even if Smartmatic did possess responsive materials, though, Defendants' requests would be improper because they have not shown any need to inspect this highly confidential and proprietary technology. Indeed, Defendants argue that they need to inspect the BMDs and source code to probe the falsity of their statements that Smartmatic rigged the election. But it is beyond dispute that Smartmatic provided voting technology for use in the 2020 Election only in LA County, and California was not even a battleground state. Moreover, all sorts of alternative sources, including the California SOS's official reports regarding the source code and its approval of the VSAP system, squarely address whether a "backdoor" was built into the source code and whether Smartmatic's technology otherwise could have flipped votes from Donald Trump to Joe Biden. Accordingly, the Court should reject Defendants' request to inspect LA County's highly confidential voting technology.

## I. Smartmatic Does Not Have Possession, Custody, or Control Of The Requested Materials.

A party may discover documents and tangible things in another party's "possession, custody, or control." Fed. R. Civ. P. 34(a). Documents and things are deemed to be within a party's "possession, custody or control" for purposes of Rule 34 if: (i) the party has "actual" possession, custody or control of them, or (ii) it has the "legal right" to obtain the materials on demand. *Prokosch v. Catalina Lighting, Inc.*, 193 F.R.D. 633, 636 (D. Minn. 2000) (citation omitted). Defendants' Motion should be denied because Smartmatic has neither actual possession of LA County's BMDs and source code, nor the legal right to obtain them.

### A. Smartmatic Does Not Have Actual Possession Of LA County's BMDs And Source Code.

It is well settled that "[a] party cannot be compelled to produce what it does not have." *List v. Carwell*, No. 18-cv-2253 (DSD/TNL), 2020 WL 5988514, at *6 (D. Minn. Oct. 9, 2020) (collecting cases). Thus, courts deny motions to compel production of documents and information where the responding party asserts in good faith that it does not actually possess the materials requested by the movant. *See id.*; *see also Edeh v. Equifax Info. Servs., LLC*, 291 F.R.D. 330, 337 (D. Minn. 2013) (denying plaintiff's motion to compel where "Equifax maintain[ed] that it [did] not have the documents requested in Requests for Production Nos. 3 and 4."). That is the case here.

MyPillow requested that Smartmatic produce, in pertinent part: (i) an exemplar of each Smartmatic product that was used to administer the 2020 Election in any jurisdiction; (ii) the source code for any Smartmatic product used to administer the 2020 Election; and (iii) any hardware or software that was used to administer the 2020 Election. (ECF No. 76-1, Ex. A, Request Nos. 1, 8, 10.) LA County is the only jurisdiction that used a product manufactured by Smartmatic and/or source code developed by Smartmatic to administer the 2020 Election. (Long Decl. ¶¶ 8-10.) In that light, the only items that are responsive to MyPillow's requests are a BMD used in LA County in the 2020 Election and the source code developed by Smartmatic for the BMDs. (*See* ECF No. 76-1, Ex. A, Request Nos. 1, 8, 10.) Smartmatic does not have possession, custody, or control, of either item.

*First*, Smartmatic does not possess the BMDs that LA County used in the 2020 Presidential Election. (Long Decl. ¶ 26.) Smartmatic manufactured the BMDs pursuant to its contract with LA County. (Bloom Decl. ¶ 3, Ex. 1.) Under the contract, the BMDs were the property of LA County upon delivery and remained its property following the 2020 Presidential Election. (Long Decl. ¶ 9; Bloom Decl. ¶ 3, Ex. 1 §§ 2.1.1, 2.3.1.) Following the 2020 Election, Smartmatic has performed maintenance on LA County's BMDs as needed, but it has not taken "possession" of them. (Long Decl. ¶ 26.) Rather, even during the maintenance, the BMDs remain in LA County's possession and are stored on property owned by LA County. (*Id.*) Thus, Smartmatic does not possess a BMD "used to administer" the 2020 election. (*See* ECF No. 76-1, Ex. A, Request No. 1).

*Second*, Smartmatic does not possess the source code or trusted build files that LA County deposited into escrow, including the trusted build file that LA County installed in the BMDs for use in the 2020 Election. (Long Decl. ¶¶ 20-21, 25.) VSAP 2.2 was the software used in the BMDs in the 2020 Election. (*Id.* ¶ 11.) VSAP 2.1 was conditionally approved by the California SOS after rigorous testing, and then days later, the SOS approved VSAP 2.2, which made minor modifications to VSAP 2.1. (*Id.* ¶ 19; Bloom Decl. ¶¶ 6-7, Ex. 4-5.) As part of the certification process, Smartmatic provided VSAP 2.1 and VSAP 2.2 to the independent testing authority, which then created a trusted build file. (Long Decl. ¶¶ 13-18.) Pursuant to California law, after VSAP 2.1 and VSAP 2.2 were conditionally approved by the SOS, LA County was required to place the approved source code and trusted build files into an escrow account. (*Id.* ¶ 20.) Then, before the election, LA County accessed the trusted build files in the escrow account and installed them in the BMDs. (*Id.* ¶¶ 22-23.)

Smartmatic has never had access to the escrow account. (*Id.* ¶¶ 20-21, 25.) In that regard, Smartmatic does not possess the files that LA County installed in the BMDs. (*Id.*) As an LA County contractor, Smartmatic has access to a database containing versions of VSAP 2.1 and VSAP 2.2 that it provided to the independent testing authority and the trusted build file that it received from the independent testing authority, but its access to the database is subject to the permission of LA County and restrictions implemented by LA County. (*Id.* ¶ 25.) Moreover, MyPillow has requested the source code that was actually "used" in the BMDs in the 2020 election. (ECF No. 76-1, Ex. A, Request No. 8).) That is the code that LA County placed into escrow and installed into the BMDs, *i.e.,* code that Smartmatic has never been able to access. (Long Decl. ¶ 23.)

Although Smartmatic does not have possession, custody, or control of the BMDs and source code that LA County used to administer the 2020 election, Defendants are not left without a remedy. Indeed, where, as here, a party does not possess the requested materials, courts encourage the discovering party to seek the materials from a third party in possession of them. *See List*, 2020 WL 5988514, at *6 ("Whatever ICBC-claims-related discovery the List Plaintiffs may have hoped to get indirectly from Defendants should have been sought directly from ICBC by subpoena or other similar process."); *Blue Spike, LLC v. Vizio, Inc.*, No. 8:17-cv-01172-DOC-KESx, 2018 WL 8646476, at *5 (C.D. Cal. July 3, 2018) (denying motion to compel source code that was not in defendant's possession, custody, or control, and instructing plaintiff "to pursue third-party discovery to obtain [it]."). Defendants have already notified Smartmatic that they intend to subpoena LA County and the California SOS for the source code used in the 2020 Election and other documentation related to VSAP and Smartmatic's role in the election. (Bloom Decl. ¶¶ 8-9, Ex. 6-7.) Accordingly, to the extent that Defendants believe they need to inspect the source code used in the 2020 Election, they can attempt procure an inspection through their subpoenas.

### B. Smartmatic Does Not Have The Legal Right To Obtain The BMDs and Source Code Requested By MyPillow.

The Court should also deny Defendants' Motion to Compel because Smartmatic does not have the "legal right" to obtain and produce LA County's BMDs and source code. *See Roark v. Credit One Bank, N.A.*, No. 16-173 (RHK/FLN), 2016 WL 11606777, at *3 (D. Minn. Dec. 1, 2016) (denying motion to compel where plaintiff failed to show that defendant had any "legal right or authority" to obtain the request information). Indeed, all of the BMDs and VSAP source code that Smartmatic produced and manufactured for LA County are the exclusive property of LA County. Moreover, the LA County/Smartmatic contract expressly forbids Smartmatic from sharing LA County's confidential information.

*First*, Smartmatic has no right under its contract with LA County to obtain the BMDs and escrowed source code. Smartmatic and LA County agreed that "anything developed, designed and/or provided by [Smartmatic] in the course of providing the Services, including but not limited to, the VSAP Solution, and all works based thereon, incorporated therein, or derived therefrom, shall be the sole property of [LA] County." (Bloom Decl. ¶ 3, Ex. 1 § 2.1.1.) Moreover, their contract provides that LA County is "*the sole owner* of all right, title and interest, including copyright, in and to all software, plans, diagrams, facilities, documentation, and tools, which are originated or created through Contractor's and its Subcontractor's work pursuant to this Contract." (*Id.* § 2.3.1 (emphasis added).) And the parties agreed that the VSAP Solution, including "any aspects, parts, or components of it . . . is owned exclusively by [LA] County." (*Id.*)

*Second*, the confidentiality provision in the LA County/Smartmatic contract makes clear that Smartmatic cannot obtain the BMDs and escrowed source code. Indeed, even if Smartmatic possessed those items, it would be expressly *barred* from disclosing them because they reflect LA County's confidential information "obtained" by Smartmatic pursuant to the agreement. (*Id.* § 7.8.1.) Smartmatic can only disclose such records or materials if a Court orders it to produce them or LA County provides its express written consent. (*Id.* § 7.8.3.) Smartmatic informed LA County about MyPillow's requests for production of LA County's BMDs and source code, and LA County said it would not make them available to Smartmatic for production to Defendants. (Bloom Decl. ¶ 16.)

Smartmatic does not have actual possession of the BMDs or source code requested by Defendants and it has no legal right to obtain them. Accordingly, the Court should deny Defendants' Motion to Compel. *See List*, 2020 WL 5988514, at *6.

## II. The Court Should Deny Defendants' Motion Because Defendants' Requested Inspection Is Not Necessary.

The Court should also deny Defendants' motion because their requested inspection of confidential voting technology is unnecessary. Defendants claim that they need this discovery to establish the truth of their statements that Smartmatic rigged the 2020 election. But disclosure of LA County's voting technology to *anyone*—let alone an individual who is under investigation for illegal conduct related to voting technology—threatens the security of elections in LA County. Moreover, alternative sources of information sufficiently address whether Smartmatic or its technology flipped votes in LA County from Donald Trump to Joe Biden. Accordingly, the Court should deny Defendants' motion for that reason as well.

### A. Courts Reject Requests To Inspect Highly Confidential Source Code When The Inspection Is Not Necessary.

Federal Rule of Civil Procedure 26(b)(1) provides that "parties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." Fed. R. Civ. P. 26(b)(1). Courts are required, however, to "limit the . . . extent of discovery otherwise allowed by these rules [if it] can be obtained from some other source that is more convenient, less burdensome, or less expensive." Fed. R. Civ. P. 26(b)(2)(C); *see also Peterson v. Seagate U.S. LLC*, No. 07-2502 (MJD/AJB), 2009 WL 3430150, at *8-9 (D. Minn. Oct. 19, 2009) (limiting discovery where the information requested could be obtained through other sources).

That principle governs the requests at issue here. Indeed, even in cases where a party's confidentiality concerns are purely commercial, "[c]ourts have held that when source code is requested not only must it be relevant and necessary to the prosecution or defense of the case but when alternatives are available, a court will not be justified in ordering disclosure." *Congoo, LLC v. Revcontent LLC*, No. 16-401 (MAS), 2017 WL 3584205, at *3 (D.N.J. Aug. 10, 2017); *Saleh v. Nike, Inc.*, No. CV 20-09581-FLA (RAOx), 2021 WL 4434352, at *2 (C.D. Cal. Aug. 16, 2021) (same); *Neo Ivy Capital Mgmt. LLC v. Savvysherpa LLC*, No. 18-mc-0094 (SRN/DTS), 2019 WL 1435058, at *6 (D. Minn. Mar. 8, 2019) (denying motion to compel all source code created by an employee because it was "highly confidential and proprietary" and plaintiff failed to show a "particularized need" for it); *see also Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 260 (S.D.N.Y. 2008) (denying motion to compel source code because plaintiff did not make a "plausible showing" that its allegations concerning defendants' source code were true).

In *Congoo*, plaintiff brought a Lanham Act claim and requested to inspect defendants' source code to show that they were involved in creating the false and misleading ads at issue in the lawsuit. 2017 WL 3584205, at *1. But the court denied plaintiff's motion to compel because: (i) plaintiff could gain an understanding of the software algorithm through alternative sources, such as testimony from defendants' employees and documentation that defendants agreed to produce; (ii) defendants' source code was "highly confidential" and disclosure would cause "irreparable harm"; and (iii) non-disclosure of the source code was safer than relying on the parties' stipulated confidentiality order. *Id.* at *4; *see also Saleh*, 2021 WL 4434352, at *2 (denying motion to compel source code because "Plaintiff has not established why he cannot obtain the information he needs by alternative means.").

### B. Defendants' Requested Inspection Of Highly Confidential Voting Technology Is Not Necessary.

The Court should deny Defendants' Motion to Compel for substantially the same reasons that the court relied upon in *Congoo*. *First*, the requested voting technology is highly confidential and disclosure would threaten LA County's election security. *Second*, alternative sources of information squarely address whether votes in LA County were compromised or "flipped."

### 1. Disclosure Of The Requested Materials Would Threaten Election Security.

In *Viacom*, the court denied plaintiff's motion to compel, in part, because Google had invested millions of dollars into research related to the source code and disclosure of it could have given its competitors an advantage. 253 F.R.D. at 259-60. Here, the consequences of disclosure are even greater because Defendants request highly confidential voting technology and Lindell, who is under investigation for crimes related to voting technology, has threatened to use discovery obtained in this case in his baseless crusade against voting technology companies.

***First***, the importance of election security is beyond dispute. The United States Supreme Court has stated that "[c]onfidence in the integrity of our electoral processes is essential to the functioning of our participatory democracy." *Purcell v. Gonzalez*, 549 U.S. 1, 4 (2006); *see also Cook Cty. Republican Party v. Pritzker*, 487 F. Supp. 3d 705, 710 (N.D. Ill. 2020) (describing the "critical importance of secure elections to a functioning democracy"). And the agencies charged with protecting the public, including the Department of Homeland Security ("DHS") and the Cybersecurity & Infrastructure Security Agency ("CISA"), recognize that "[e]lections play a vital role in a free and fair society and are a cornerstone of American democracy" and that "[a] secure and resilient electoral process is a *vital national interest* and one of [their] highest priorities."[2]

[2] *Election Security*, DEPARTMENT OF HOMELAND SECURITY, *available at* https://www.dhs.gov/topics/election-security (last visited Feb. 15, 2023) (emphasis added); *Election Infrastructure Security*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, *available at* https://www.cisa.gov/election-security (last visited Feb. 15, 2023) (emphasis added).)

For its part, LA County has stated that "[e]lection security is a matter of grave concern" because, among other reasons, "[a]ccusations of election fraud—including accusations directed against voting equipment and voting systems—without sufficient proof have been widely made and unfortunately widely believed." (Bloom Decl. ¶ 10, Ex. 8, M. Owens Declaration ¶ 7.) Further, any county, much less one containing 10 million people, must "thoroughly protect the security of its election processes and equipment." (*Id.* ¶ 8.) To that end, LA County "attempts to thoroughly protect the security of its election processes and equipment by using a system of multi-layered security protocols, including maintaining the security of physical devices and software." (*Id.*) Thus, Defendants cannot reasonably contend that election security is not a compelling concern.

***Second***, disclosure of the BMDs and source code to Defendants in this case would threaten election security because Smartmatic and the Court can have no assurance that Defendants will maintain the confidentiality of the requested materials. Defendants argue that the parties' stipulated confidentiality order allays any such concerns. (ECF No. 75 at 11-12.) But even when parties have agreed to a protective order, courts have erred on the side of "nondisclosure" of confidential and proprietary source code when disclosure could cause irreparable harm and the moving party has failed to establish that it needs to review the information. *See Viacom*, 253 F.R.D. at 260 (noting that the parties' stipulated confidentiality order was "careful and extensive, but nevertheless not as safe as nondisclosure"); *Congoo*, 2017 WL 3584205, at *4 ("Assuming . . . that the source code is relevant, the Court finds that its highly confidential nature is such that it cannot be adequately safeguarded by a Discovery Confidentiality Order and therefore outweighs the need for production.").

In this case, the facts weigh even more in favor of nondisclosure because Defendants are a threat to publicly disclose the requested materials. Indeed, in addition to propagating a disinformation campaign for over two years designed to undermine the result of a fairly contested U.S. Presidential election, Lindell has stated that defending a lawsuit against a voting technology company would "make [his] day" because "then they would have to go into discovery, and that would make my job a lot easier."[3] According to Lindell, with discovery, "[i]t'll be faster for me to get to the evidence, ***and to show the people in the public record the evidence*** we have about these machines . . . ***I will not stop until every single person on the planet knows*** . . . what these machines did to us." *Id.* (emphasis added). Similarly, Lindell told ABC News he was "so happy" when he was sued by Smartmatic's competitor, Dominion, because "it [would] enable him to demand internal company documents through the legal discovery process."[4]

Lindell is also being investigated by the FBI for potential crimes related to accessing voting machine technology. On September 7, 2022, Judge Leung issued a warrant for the search of Lindell's person and seizure of his personal cell phone in

[3] Asawin Suebsaeng, Lachlan Cartwright, & Adam Rawnsley, *Dominion Says It Will Sue MyPillow CEO Mike Lindell Over Election Fraud Claims*, The Daily Beast (Feb. 16, 2021), https://www.thedailybeast.com/dominion-says-it-will-sue-mypillow-ceo-mike-lindell-over-election-fraud-claims (last visited Feb. 15, 2023).

[4] Olivia Rubin & Soo Rin Kim, *Voting machine company sues pro-Trump pillow man over false election claims*, ABC News (Feb. 22, 2021, 11:07 AM), https://abcnews.go.com/US/voting-machine-company-sues-pro-trump-pillow-man/story?id=76043949 (last visited Feb. 15, 2023).

connection with unauthorized access of a Dominion voting system in Mesa County, Colorado.[5] Judge Leung found probable cause for federal agents to search Lindell's phone for information "relating to damage to any Dominion computerized voting system, including any impairment to, or attempt to impair, the integrity or availability of data, a program, a system, or information" as well as information related to "any attempted or successful misappropriation, theft, conversion, transfer, or exfiltration of any proprietary hardware, software, or other data."[6]

Undeterred by the FBI's investigation, Lindell has continued his public crusade against Smartmatic and its competitors. He routinely states that he "can't wait for the day we melt down those machines and turn them into prison bars."[7] And, just weeks ago, Lindell conducted an interview in a "claw machine" on Jimmy Kimmel Live so he could further perpetuate the falsehood that Smartmatic and its competitors rigged the election.[8]

Based on Lindell's well-documented desire to harm Smartmatic, and his plan to use discovery to advance his own goals outside of this litigation, the Court cannot be certain that the stipulated confidentiality order will adequately protect the confidentiality of LA County's voting technology. Accordingly, nondisclosure is the safest way to

[5] *See Lindell v. United States*, No. 0:22-cv-2290 (D. Minn. 2022), ECF No. 6, *available at* https://lawandcrime.com/2020-election/doj-seized-mike-lindells-phone-to-search-for-evidence-of-identity-theft-and-computer-crimes-warrant-reveals/ (last visited Feb. 15, 2023).

[6] *Id.* at 4–5, ¶¶ 2(a), (g).

[7] *See, e.g.,* Natalie Musumeci, Warren Rojas, & Cheryl Teh, *Supreme Court won't let MyPillow CEO Mike Lindell dodge Dominion's $1.3 billion defamation lawsuit* (Oct. 3, 2022), https://www.businessinsider.com/supreme-court-rejects-mike-lindell-mypillow-dominion-lawsuit-2022-10 (last visited Feb. 15, 2023).

[8] *Jimmy Kimmel Live* (ABC television broadcast Jan. 31, 2023), *available at* https://www.youtube.com/watch?v=vGlDEbZvwLI. (last visited Feb. 15, 2023).

protect the confidentiality of LA County's VSAP system. *See Viacom*, 253 F.R.D. at 260; *Congoo*, 2017 WL 3584205, at *4.[9]

### 2. Other Sources Of Information Adequately Address The Issues That Defendants Seek To Probe.

Defendants argue that they need to inspect the BMDs and source code to test the truth or falsity of their defamatory statements that Smartmatic's technology was: (i) "compromised or hacked" to steal the 2020 election; (ii) connected to the Internet during the 2020 election; and (iii) designed to steal elections. (ECF No. 75 at 6-9.) Although Defendants claim that they possess "some information" to support those statements, they have never disclosed it in their defamatory publications or in discovery. (*See id.* at 10.) Nor should they be permitted to inspect BMDs and source code to find such evidence because alternative sources of information—including publicly available information, documents that Smartmatic has agreed to produce, and depositions of Smartmatic witnesses— will all sufficiently address the falsity (or "truth") of Defendants' defamatory statements. *See Peterson*, 2009 WL 3430150, at *8-9; *Saleh*, 2021 WL 4434352, at *5; *Congoo,* 2017 WL 3584205, at *4.

***First***, Defendants can review the sources related to the rigorous testing mandated by the California SOS before LA County's VSAP technology could be certified for use in the 2020 Election. Pursuant to California law, the SOS and/or independent testers

[9] Defendants' citations to *Northbrook Digital, LLC v. Vendio Servs.*, 625 F. Supp. 2d 728, 744-45 (D. Minn. 2008) and *Nutratech, Inc. v. Syntech Int'l, Inc.*, 242 F.R.D. 552, 555-56 (C.D. Cal. 2007) are inapposite because neither case involved a request for confidential voting technology by parties who publicly declared their intent to use discovery to expose a "fraudulent" U.S. Presidential election.

working at its direction, performed all sorts of tests on the VSAP system, including security testing that includes a full source code review and penetration testing. (Bloom Decl. ¶ 6, Ex. 4.) The results of the testing performed by the SOS's independent testing authority are publicly available. (*Id.* ¶¶ 4-5, Ex. 2-3.) These reports provide comprehensive analyses of the code, including the security of it and whether any "backdoors" were built into it that could have been used to "flip" votes from Donald Trump to Joe Biden. (*Id.* ¶ 4, Ex. 2 at 5 (independent testing authority reviewed whether VSAP 2.1 included "embedded, exploitable code").) Defendants are well-aware of these reports and even cited them in the subpoena they plan to serve on the SOS. (Bloom Decl. ¶ 9, Ex. 7 at 5.)

***Second***, alternative sources of information show other security requirements that the California SOS imposes before certification. For example, the SOS requires that voting technology be "air-gapped" such that it cannot be connected to the internet. (Bloom Decl. ¶ 6, Ex. 4 ¶ 4.) The independent testing authority's report confirms that the VSAP System is air-gapped. (*Id.* ¶ 5, Ex. 3 at 36 (noting that the VSAP solution is "on an air-gapped network").) Other sources also show that, after Smartmatic developed the source code, an accredited independent testing authority oversaw the creation of the trusted build file that LA County would submit to the SOS for approval and subsequently install in the BMDs. (Long Decl. ¶ 16.) Then, the independent testing authority created an immutable hash value that uniquely identifies the code it built. (*Id.* ¶ 17.) After creation of the hash value, any modification to the file would result in that file returning a different hash code, allowing vendors and elections officials to compare hash values and confirm that the voting system and its source code has not been altered. (*Id.*)

***Third***, alternative sources of information discuss the additional safeguards that LA County and SOS applied after conditional approval of Smartmatic's technology to ensure the security of the election. These safeguards included the requirement that LA County deposit the approved source code and trusted build file into an escrow account that not even Smartmatic could access. (Bloom Decl. ¶ 6, Ex. 4 ¶ 6.) Additionally, LA County used encryption keys for VSAP. (Long Decl. ¶ 24.) These encryption keys, which only LA County possesses, ensure that if the software loaded onto the hardware is not identical to the trusted build file, the software will crash and the machine will not be usable. (*Id.*)

***Fourth***, Defendants can probe whether Smartmatic's technology could have been used to flip votes or hacked based on sources of information concerning BMDs. These sources will show that a BMD merely prints a paper ballot reflecting a voter's choices. (Bloom Decl. ¶ 11, Ex. 9, VSAP Final Report at 8, ¶ 12, Ex. 10, BMD Ballot Security.) All voters in LA County who used a BMD manufactured by Smartmatic to cast their vote had an opportunity to confirm that the printed ballot accurately reflected their choices before their paper ballot was deposited into the Integrated Ballot Box. (*Id.* ¶ 12, Ex. 10, ¶ 13, Ex. 11, VSAP Use Procedures at 9.) A Tally System that was not manufactured or designed by Smartmatic was then used to tabulate the votes. (*Id.* ¶ 11, Ex. 9 at 8-9.). All of this information is available to Defendants and answers the question as to whether Smartmatic's technology could have rigged the election.

***Fifth***, Defendants can review vote count data to assess whether Smartmatic's technology could have been used to rig the election. The only hardware and software manufactured by Smartmatic and used in the 2020 Election were used in LA County. (Long Decl. ¶¶ 8-10.) California is not a battleground state—President Biden received 63.5% of the vote, as compared to 34.3% for President Trump. (Bloom Decl. ¶ 14, Ex. 12, 2020 CA Voting Results at 5.) President Biden received over 5 million more votes than President Trump in the State of California. (*Id.*). Only approximately 4.2 million votes were even cast in LA County. (*Id.* at 1.) Thus, data available to Defendants shows the extent to which technology manufactured by Smartmatic could have flipped the State of California from Donald Trump to Joe Biden.

Data concerning the proportion of the electorate in LA County that voted for Donald Trump in 2016 and in 2020 is also available to Defendants and is probative of the falsity of their defamatory statements. In the 2016 Presidential Election, in which Smartmatic's voting technology was not used, the Democratic candidate, Hillary Clinton, received 71.8% of the LA County vote, and the Republican candidate, Donald Trump, received 22.4% of the vote. (Bloom Decl. ¶ 15, Ex. 13, 2016 CA Voting Results at 17.) In the 2020 Election, in which Smartmatic's BMDs and source code were used, President Trump increased his vote count to 26.9% of the vote. (Bloom Decl. ¶ 14, Ex. 12, at 3.)

***Finally***, alternative sources of information show that federal and state officials confirmed that Smartmatic did not rig or hack the election. Public statements by federal and state officials, including William Barr, the Attorney General of the United States during the Trump Administration, provide that there was no evidence that anyone, let alone Smartmatic, committed a fraud that undermined the result of the 2020 Election. (Compl. ¶¶ 57-65.)

In the face of that information, Defendants cannot reasonably claim that they need to inspect the BMDs and source code to determine whether Smartmatic rigged the election, whether Smartmatic's technology was designed to rig the election, and whether it was connected to the internet. Defendants have failed to cite a shred of evidence during their 2-year disinformation campaign or in discovery that Smartmatic committed the crimes they attributed to it. They should not be permitted to now perform an invasive inspection of LA County's confidential voting technology. *See Peterson,* 2009 WL 3430150, at *8-9; *Saleh*, 2021 WL 4434352, at *5; *Congoo,* 2017 WL 3584205, at *4.

Defendants' arguments to the contrary are meritless. ***First***, Defendants misconstrue the nature of their false statements in order to expand the scope of discovery. (ECF No. 75 at 7-9.) They claim that they need to inspect the BMDs and source code to probe whether they were "susceptible" to an attack and whether "security vulnerabilities" exist. (*Id.*) Smartmatic has not alleged, though, that Defendants merely claimed that Smartmatic's technology was *vulnerable* to an attack. Rather, Smartmatic has alleged that Defendants defamed it by repeatedly stating that Smartmatic did, in fact, rig the election. (*See, e.g.,* Compl. ¶ 170.) The alternative sources of information identified by Smartmatic sufficiently address that issue and the truth or falsity of all other false statements alleged in Smartmatic's Complaint. Moreover, even if "vulnerabilities" in Smartmatic's software were relevant, the reports prepared by the independent testing authority sufficiently address that issue. (Bloom Decl. ¶ 4, Ex. 2 (discussing the findings of the independent testing authority's "Software Code Vulnerability Review").)

***Second***, Defendants argue that "Mr. Lindell's possession of some information to prove the truth of his statements does not prevent him from gathering additional or supporting evidence." (ECF No. 75 at 10.) Smartmatic is unaware of any evidence in Lindell's possession that supports his defamatory statements. Nor could any such evidence exist because his statements were wholly false, and he knew that they were false or acted with reckless disregard for the truth when he made them. (*See* Compl. ¶¶ 181-345.) Regardless, as discussed above, whether or not Lindell believes that he already possesses evidence that his statements regarding Smartmatic are true, he is not entitled to inspect LA County's highly confidential BMDs and source code.[10]

## CONCLUSION

Smartmatic does not possess the requested BMDs or source code used in the BMDs for the 2020 election in LA County. For that reason, alone, the Court can deny Defendants' Motion to Compel. Additionally, the Court should deny Defendants' Motion to Compel because they have not established that they need to inspect these highly confidential materials instead of relying upon alternative sources of information.

[10] MyPillow has requested that Smartmatic "produce" the BMDs and source code. (ECF No. 76-1, Ex. A.) Even if the Court grants Defendants' Motion to Compel, it should only permit Defendants to *inspect* the requested materials after the parties agree upon an inspection protocol.

Dated: February 16, 2023

Respectfully submitted,

/s/ *Michael E. Bloom*
Christopher K. Larus
Minnesota Bar No. 0226828
CLarus@robinskaplan.com
William E. Manske
Minnesota Bar No. 0392348
WManske@robinskaplan.com
Emily J. Tremblay
Minnesota Bar No. 0395003
ETremblay@robinskaplan.com
**ROBINS KAPLAN LLP**
800 LaSalle Avenue, Suite 2800
Minneapolis, MN 55402
Telephone: (612) 349-8500

J. Erik Connolly (admitted *pro hac vice)*
EConnolly@beneschlaw.com
Illinois ARDC No. 6269558
Nicole E. Wrigley (admitted *pro hac vice)*
NWrigley@beneschlaw.com
Illinois ARDC No. 6278749
Michael E. Bloom (admitted *pro hac vice*)
MBloom@beneschlaw.com
Illinois ARDC No. 6302422
Julie M. Loftus (admitted *pro hac vice*)
JLoftus@beneschlaw.com
Illinois ARDC No. 6332174
**BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP**
71 South Wacker Drive, Suite 1600
Chicago, IL 60606
Telephone: (312) 212-4949

*Attorneys for the Plaintiffs*