No.

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

IN RE TRUE THE VOTE, CATHERINE ENGELBRECHT,
And GREGG PHILLIPS

Mandamus from the United States District Court
for the Southern District of Texas

Case No. 4:22CV3096, *Konnech Inc. v True The Vote, Catherine Engelbrecht And Gregg Phillips*

MICHAEL J. WYNNE
Attorney at Law
Texas State Bar No 0078529
Telephone: (281) 450-7403
mwynne@gwafirm.com

CAMERON POWELL*
Attorney at Law
DC Bar No 459020
Telephone: (832) 390-2644
cpowell@gwafirm.com

JAMES L. TURNER
Of Counsel
Texas State Bar No. 20316950
Telephone: (713) 305-5457
jturner@gwafirm.com

**Pro Hac Vice pending*

Attorneys for Petitioners

No. _____

IN RE TRUE THE VOTE, INC., CATHERINE ENGELBRECHT,
And GREGG PHILLIPS

Mandamus from the United States District Court
for the Southern District of Texas
Case No. 4:22CV3096, *Konnech Inc. v True The Vote, Inc., Catherine Engelbrecht And Gregg Phillips*

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Rule 28.2.1 have an interest in the outcome of this case. These representations are made in order that the judges of this court may evaluate possible disqualification or recusal. The judge below was the Honorable Kenneth Hoyt.

Petitioners:	Catherine Engelbrecht Phillip Gregg True the Vote, Inc.
Attorneys for Petitioner:	Michael J. Wynne Cameron Powell James L. Turner GREGOR WYNNE ARNEY, PLLC 909 Fannin Street, Suite 3800. Houston, Texas 77010 mwynne@gwafirm.com cpowell@gwafirm.com jturner@gwafirm.com

Brock C. Akers
The Akers Law Firm
3401 Allen Parkway, Suite 101
Houston, Texas 77019
bca@akersfirm.com

John C. Kiyonaga
Law Offices of John Kiyonaga
600 Cameron Street
Alexandria, Virginia 22314
john@johnckiyonaga.com

Respondent: Konnech Inc.

Attorney for Respondent:

Constantine Z. Pamphilis
KASOWITZ BENSON TORRES LLP
Wedge International Tower
1415 Louisiana, Suite 2100
Houston, Texas 77002
dpamphilis@kasowitz.com

/s/ Michael J. Wynne
Attorney of Record for Catherine Engelbrecht, Gregg Phillips, and True the Vote, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

RELIEF SOUGHT AND JURISDICTION

Catherine Engelbrecht and Gregg Phillips, Petitioners herein and Defendants below, file this application for mandamus from the district court (Hoyt, SDJ)'s order finding them in civil contempt of court in Case No. 4:22CV3096, Konnech Inc. v True the Vote, Inc., et al. The jurisdiction of the district court was invoked under 28 U.S.C. §§ 1331 and 1367(a). This Court's jurisdiction is invoked under 28 U.S.C. § 1651.

STATEMENT OF THE ISSUE

WHETHER THE DISTRICT CLEARLY ERRED AND ABUSED ITS DISCRETION WHEN IT FOUND PETITIONERS IN CONTEMPT OF COURT AND ORDERED THEM DETAINED.

STATEMENT OF THE CASE

A. Course of proceedings and disposition below

On September 12, 2022, Plaintiff Konnech Inc. (Konnech) filed a Complaint against True the Vote Inc. (TTV), Catherine Engelbrecht, and Gregg Phillips (Defendants), and an Application for an *ex parte* Temporary Restraining Order (TRO), whose alleged *ex parte* necessity was based on fatally flawed misunderstandings of Defendants' public statements, (Dkt 1, 5). The Complaint and

the TRO are based on alleged violations of 18 U.S.C. § 1030 et seq., the Computer Fraud and Abuse Act, and Texas Remedies Code § 143.002.

On September 21, 2022, Konnech filed a Motion for Order to Show Cause as to Contempt against Defendants. (Dkt. 16). The district court set a show cause hearing on October 17, 2022. (Dkt. 33). It conducted the show cause hearing on October 27, 2022. The court continued the hearing until October 31, 2022, and concluded it that day. It ordered defendants Catherine Engelbrecht and Gregg Phillips to be detained until they fully complied with the Court's Order as set out in the TRO. (Dkt. 51).

B. <u>Statement of Facts</u>

This contempt proceeding is founded on Defendants[1] grossly misunderstood public statements, by Plaintiff and the district court, having to do with both (1) ***Chinese Server Data*** – sensitive data one defendant, Gregg Phillips, witnessed on a TV monitor in a Dallas hotel room in late January 2021 – which data is the sole subject of Plaintiff's claims of computer fraud – and (2) ***Election Breach Information*** – summary information about the resulting election system

[1] In an October 6 hearing, Plaintiff's counsel said, "This TRO . . . was based on . . . public statements [Defendants] had made, threats to disclose information." Doc 30 TR at 13-15; *see also* Plf's Motion for TRO at 3 ("The Court should consider this Motion ex parte, because . . . Defendants may follow through on their threats to publicly release the data . . .") (emphasis added).

vulnerabilities, all publicly available, which Defendants wished to convey to the public as a warning.

As a result of its misunderstanding of Defendants' modestly technical descriptions, Plaintiff has misunderstood this case to be in some way about hacking, or the Computer Abuse and Fraud Act, or about disclosure of sensitive data (whether of Plaintiff or individuals). All of these assumptions are incorrect. But the district court perpetuated that misunderstanding in ordering Defendants to make disclosures to Plaintiff that were alternatively impossible, inappropriate, or legally irrelevant.

Based entirely on its demonstrably flawed assumptions, Plaintiff inappropriately *ex parte* obtained a TRO seeking discovery outside standard civil procedure.[2] Perhaps goaded by Plaintiff's characterizations of this case as being about "election denialism", the Court took the unusual step of issuing a TRO that compelled affirmative relief from Defendants (1) in the absence of any evidence from Plaintiff, (2) based on demonstrable mischaracterizations of Defendants' public statements, (3) without permitting Defendants to proffer all relevant evidence, and

---

[2] This court's issuance of a highly unusual TRO did not arise from extraordinary factual support, but rather the reverse. The motion for a TRO had been supported solely by the affidavit of Eugene Yu, founder and CEO of Konnech. Additionally, the affirmative portions of the TRO, by supplanting the typical discovery process, have prejudiced Defendants by forcing disclosures unprotected by the right to object and seek confidentiality attendant to civil discovery.

(4) based on the incorrect conclusion that a person who witnessed Chinese Server Data not shown to belong to Plaintiff somehow "accessed" a "protected computer" of Plaintiff. Highlighting the hazards of *ex parte* hearings, the district court uncritically accepted Plaintiff's counsel's incorrect statement that Defendants "admitted hacking and theft of financial and other sensitive personal data of purportedly 1.8 million U.S. poll workers allegedly from a Konnech protected computer." Plf's Mot. for TRO at 1.

Following the *ex parte* appearance by counsel for Konnech on the same day it filed its Complaint and motion for injunctive relief, whose merits and supposed urgency were both based on Plaintiff's grave misconceptions about the types of information Defendants had spoken of, this Court issued the TRO, which holds, in pertinent part, that the defendants are enjoined from:

- "accessing", "using", or "disclosing" "Konnech's protected computers" and data; or
- deleting or destroying same,

Defendants pledged to comply with this portion of the order soon after. But the TRO also compels Defendants to disclose:

- the identity of any individual involved in "accessing Konnech's protected computers",

- the manner, means and time of "accessing" such computers, and
- the identity of any individual to have received said data.

TRO (Doc 9 at paras. i through vii).

In a hearing on October 6, the court forced Defendants' prior counsel to reveal to Plaintiff, in open court and against their protests, the name of one of the confidential informants to the FBI who happened to be in the Dallas hotel room. Defendants subsequently disclosed information responding to the remainder of the court's order, substantially complying with the order and omitting *only* to publicly name a *second* confidential informant ("the Second Informant") (1) who was not alleged to have "accessed" any computers in this case, let alone Konnech's, (2) whom Plaintiff had failed to establish had relevant evidence, and (3) whose personal safety the district court said it did not care about.

On October 27, 2022, at a show cause hearing the Court held Defendants in civil contempt for failing to identify the third of three individuals. Aside from the fact that the individual in question had not "accessed" a "protected computer" known to belong to Konnech, Defendants' hesitation in disclosing another confidential informant was due, in part, to their attempts to grapple with the nature of Plaintiff's and the court's misunderstandings, in part because Defendants were concerned about blowing the cover of confidential informants to the FBI and putting them at personal

risk, and in part because their original counsel. But their hesitation was not, as Plaintiff and the court characterized it, contemptuous.

Crucially, in the October 6 hearing, Plaintiff misrepresented the disputed nature of their conclusions about Defendants' statements, saying, "[T]here is Fifth Circuit precedent that says that the Court can consider a preliminary injunction without live testimony *so long as there is no genuine issue of material fact*." DOC 30 TR at 9 (emphasis added). But there is a genuine issue of material fact here -- consistent mischaracterizations by Plaintiff's counsel about the nature of what Phillips saw (American poll worker data on a server located in China) and what Defendants have said they would do (report the fact of such data being breached and available in China – not the data itself).

1. Defendant Phillips Witnessed a Portion of the Chinese Server Data

Defendant Phillips witnessed, on a TV monitor in a Dallas hotel room, enormous amounts of data (he was told 350TB) on a server located in China, some of it including sensitive data on American poll workers.[3] Also present were the

---

[3] To clear up some confusion, the data did not include 1.8 million poll workers:

Q. How many poll worker records were there?

A. There were 1.8 million records in that particular system. But it wasn't just -- the way that they configure everything, it wasn't just poll workers. It was election judges. There was all sorts of

person who accessed the data, Michael Hasson, whose name was revealed during the hearing of October 6, and the third individual. Some of the data appeared to have come from, or been taken from, Plaintiff Konnech.

But while the court's order to show cause is entirely about this data, unrebutted testimony shows that Defendants did not themselves access the Chinese Server Data, did not download or copy it, do not otherwise possess it, and have never stated they would reveal it to anyone.

a. Defendants Did Not Download the Chinese Server Data

> Q. Did any -- forgive me if I get the terminology -- but did any downloading occur in your presence in that hotel room when the -- whatever was up on the TV screen was up on the TV screen -- was any access happening?
>
> A. No.

Doc 47 TR, p.32 (Phillips answering).

b. No Defendant Has a Copy of the Chinese Server Data

> Q. Do you have, in your possession, a copy of this electronic information that was displayed on that screen in the hotel room in Dallas?
>
> A. No, sir.
>
> Q. Does Ms. Engelbrecht have a copy?

---

entries for the equipment; different software they used. There were millions of entries in the spreadsheet.

Doc 47 TR at 59 (statement of Phillips).

A. No.

Q. Does True The Vote have a copy?

A. No, sir.

Q. Does anybody associated with True The Vote have a copy?

A. No, sir.

Q. Did you ever have a copy of the electronic data on your computer or otherwise in your individual possession?

A. No.

Doc 47 TR, pp. 33-34 (Phillips answering).

On October 6, Defendants' prior counsel had already informed the court that the Chinese Server Data was something Phillips had only seen, and did not possess:

MR. BREWER: Your Honor, seeing it [data] and possessing it [data] are two different things.

THE COURT: Well, it may not be and it may be.

(DOC 30 TR at 37-38).

c. Defendants Did Not Witness Hacking or Means of "Access"

In unrebutted testimony, Defendant Phillips also made clear that what he saw in the hotel room was not "accessed" at that time. Rather, he was shown the results of the access on the TV monitor:

Q. What, if anything, was your impression on the temporal relationship -- that is the time relationship between when you walked into the hotel room and whenever whoever it was downloaded the information or data that appeared on the TV monitor that you saw?

A. It took about 20 minutes to get his computer hooked to the television screen. He had a problem with the cord that needed to hook into the hotel screen. Once he pulled it up, *he went straight to his files that he was showing me*.

Q. Was it your impression that information was actively being retrieved at that moment in the hotel room, or was it your impression that that had already been done, and he was showing you something that had been done in the past?

A. *I think it was being done in the past*. He certainly wouldn't have been -- *there wouldn't have been enough bandwidth at the hotel to download that kind [350TB] of data*.

Doc 47 TR at 32-33 (emphases added).

Defendants have also made clear exactly why they could not help Plaintiff – as it demanded in its supposedly urgent motion for a Temporary Restraining Order – with its serious security problems. Because the uncontroverted testimony is that Phillips did not know how the Chinese Server Data had been accessed:

THE WITNESS: *I don't know how it was accessed*. I know it was accessed because I saw it, and I subsequently learned that the information had become important to the FBI. [As to] when, given the size of the data that I understand was downloaded, it was somewhere in the 350-terabyte range, and was downloaded over approximately three months in the first quarter of 2021.

Doc 47 TR at 35-36.

c. Defendants Did Not Provide the Chinese Server Data to Anyone

In unrebutted testimony, Defendants also made clear who gave the Chinese Server Data to the FBI – and it was not Defendants:

Q. And so how was the data sent from Mr. Hasson to the FBI?

A. They have a method to transmit large chunks of data directly to them.

Q. What's that method?

A. I didn't do it. You'd have to ask Mike.

Q. Were you involved in it being done?

A. No.

Q. Did you see it being done?

A. No.

Q. Who told you it was done?

A. The FBI.

Doc 47 TR at 54-55 (statement of Gregg Phillips).

In the same podcasts Plaintiff has cited without understanding, Phillips has also explained unrefuted information about the China-based server that should have prevented the district court from attempting to make Defendants responsible for Plaintiff's own security problems in China: "Important keynote here, guys, for everyone ... We didn't steal anything. They left it open. *The database was a MongoDB database that they left open*. … There were no tools used to break in."[4]

---

[4] https://rumble.com/v1hz1jr-heres-how-theyll-try-to-steal-the-midterms-gregg-phillips-interview.html at 36:20 (emphases added)

The second type of information, or data, in this case is about the basic *fact* of the breach of American poll workers' data, which we will call Data Breach Information. This is the only information or data that Defendants "accessed", possessed, or wanted to disclose.

2. Data Breach Information

The Data Breach Information includes the general *fact* that sensitive data on American poll workers was being stored on a computer server located in China. The Data Breach Information consists of the publicly available fact that election-related domain names hosted by Konnech on behalf of American cities were being hosted on the same China-based server as its American poll worker data, as was Konnech's URL app.konnech.com (meaning that any data that ran through its apps ran through the insecure server in China), and, apparently, what appeared to be websites for the Chinese election system (e.g., 2dmeeting.com and 2dmeeting.cn).

Exhibit 1 shows a screenshot from the publicly available website Binary Edge, which provides information on computer servers around the world. It shows the server information for Konnech-owned domain name Vote4Fairfax.com, a website run on behalf of Plaintiff's client Fairfax County, Virginia, which Defendants confirmed was registered to Konnech before the domain name's ownership information (aka WHOIS information) was recently concealed. The Binary Edge

screenshot, taken before someone changed the server to one located in the U.S, reveals several key facts:

- The screenshot was taken sometime shortly after December 29, 2020.
- The domain name Vote4Fairfax.com was hosted in China, specifically, on Unicom, one of three "backbones" of the Chinese Internet, *which is owned by the Chinese government*. *See* https://en.wikipedia.org/wiki/China_Unicom
- The computer server has IP address 101.66.244.52.
- The same server hosted many other domain names – and their data – operated by Konnech on behalf of its American clients, such as the city of Boston (Vote4Boston.com), the city of Hillsborough (Vote4Hillsborough.net), and others.
- Server 101.66.244.52 also hosted apps.konnech.com, as well as all the data on applications used by Konnech customers who access apps.konnech.com

Exhibit 2 shows that the same domain names, as well as Konnech's PollChief.com website and a few more domain names that Konnech operates on behalf of clients in Detroit and Lake County, have been belatedly moved to a server based in the United States. *See* Ex. 2 (accessed on November 1, 2022). It is *this* Data Breach Information that Defendants said, in their podcasts and The Pit event and

other media, they wished to reveal to the public. This information does not belong to Plaintiff, was not accessed from them, is not defamatory, and is within Defendants' First Amendment rights to speak about.

3. The Missed Opportunities in the Court Below

In fact, had the district court subjected Plaintiff's testimony to cross-examination, consistent with due process, the court could have determined whether Plaintiff does indeed own the above-named domain names, and whether it was Plaintiff who moved the domain names from the server in China to the one in the United States. If Plaintiff does own the domain names or did move them from an insecure server in China to a server in the United States, then its entire motion for contempt, and its argument that it needs immediate injunctive relief in the form of Defendants helping it to understand its server's "breach", could have been denied. Why? Because Plaintiff *knew* its information was on a server in China, and Plaintiff did not require the names of private individuals in order to secure its data, as Plaintiff insisted in its overheated and *ex parte* Motion for TRO. Lacking such urgency, the court's holding of the *ex parte* proceeding was itself inappropriate. And it made no sense for the court to order Defendants to tell Plaintiff what it already knew, nor to arbitrarily incarcerate them for a good-faith disinclination to disclose the names of

confidential informants who could have told them what they already knew: that they were hosting their domain names and data on a server in China.

The court did not allow Defendants to explain the crucial distinctions at issue here. It did not appear to appreciate the distinctions – admittedly somewhat technical in nature – when Defendants offered them. Witness the court's questioning of Phillips regarding the data – the Chinese Server Data – of American citizens he saw that night in the Dallas hotel room:

> THE COURT: And you saw that there were bank accounts?
>
> THE WITNESS: There were bank accounts.
>
> THE COURT: You saw the names of the individuals?
>
> THE WITNESS: Yes, sir.
>
> THE COURT: You saw their Social Security numbers?
>
> THE WITNESS: Yes, sir.
>
> THE COURT: And you then said: We're going to post this on a public domain?
>
> THE WITNESS: No, sir. There is two different datasets.
>
> THE COURT: Well, I'm not -- *I don't care about the datasets*. You know what I am describing.

"It's unrelated," Defendant Phillips began, because he did in fact know what the court was describing, but the court cut him off before he could explain the crucial distinction. *See* Doc 47 TR [5]at 97, lines 3-17 (emphasis added).

This was not Defendants' only attempt to ensure the court was informed about the fundamental issues -- and what they had and had not said they witnessed, possessed, or would disclose – before it issued the contempt citation:

> THE COURT: Okay. Do you recall making a statement on the podcast to the effect that *you were going to create a website and would load the -- this data that you saw onto the website* for the people who would want to visit that site?

Note, again, that Defendants' podcast and website both relate to the open-source, publicly available *Election Breach Information*, not the Chinese Server Data.

> THE WITNESS: No, sir. That's not true.
>
> THE COURT: I'm asking you. This is what you said -- or what your podcast said.
>
> THE WITNESS: *My podcast was referring to something we called the ripcord*. The ripcord was related to an app called Open.INK, I-N-K. We were going to put the -- we do all sorts of other research. *We do a lot of open-source research*, meaning Googling around and trying to find things. But *we also do geospatial research*.

(DOC 47 TR at 93-94 (emphases added). In other words: Election Breach Information.

---

[5] DOC refers to the district clerk's docket; the docket number follows; TR refers to the transcript.

4. Defendants' Actual Public Statements About Public Records

Plaintiff cites Defendants' public statements in its Motion for TRO:

> In the summer of 2022, Defendants advertised an event they dubbed "The Pit," scheduled for August 13, 2022, at which they claimed they would disclose "devastating" information …

Mot. for TRO at 4. Plaintiff includes, ostensibly as proof, a screenshot of a social media post, by a third-party, that does nothing but illustrate what is clearly Election Breach Information, none of it including any confidential information of Plaintiff or private individuals:

In the October 6 hearing, Defendants' counsel explained to the district court that *Plaintiff denies any "breach" of its servers*, which should have alerted both

Plaintiff and the court that the server, in China, that was easily breached by Mike Hasson, is not the same as the servers Konnech maintained in the United States:

> MR. AKERS [reading from web content from Konnech.com]: "True the Vote claims to have downloaded personal data on 1.8 million poll workers early in 2021 from an unsecured Konnech server in Wuhan, China."
>
> "Truth: Konnech thoroughly investigated True the Vote's claims and found no evidence whatsoever of any breach of our systems or Konnech data anywhere in the world."

DOC 30 TR at 32-33.

In the "Patriots and Prophets" podcast that Plaintiff cites as Exhibit A-1[6], Defendant Phillips further alerted Plaintiff, and the court below, about Defendants' open-source Election Breach Information. He said that Defendants had discussions with the FBI "in January of 2021, related to some information that we acquired from an *open source research project* that we were doing." (emphasis added)

Regarding Plaintiff's PollChief software and its use by election jurisdictions around the country, Phillips stated, in another podcast[7], that co-Defendant "Catherine [Engelbrecht] started doing *open records requests* and started learning a

---

[6] https://rumble.com/v1h1pj9-rumble-only-prophets-and-patriots-episode-20-with-gregg-phillips-and-steve-.html
[7] https://rumble.com/v1hz1jr-heres-how-theyll-try-to-steal-the-midterms-gregg-phillips-interview.html at 00:33:14.530 (statement of Gregg Phillips).

little more about these contracts and a little more about it. As we dug into *using some open source tools* that help you track these things." (emphases added)

In the same podcast, Phillips went on, "One [open source tool] called Binary Edge, we realized that there's one particular IP address where all of these soft -- and basically this company [Konnech] created a software [PollChief] that manages elections. It manages all of the information, human information, facility-based information. It manages the RFID codes on the machines, everything there is to know about an election. It manages the hours that people work in these elections. And all of this data rolls up into, let's just say it's in Fairfax County, Virginia, Vote4Fairfax.com and then Vote4Boston.com, [and Vote4La.com]. And all over the country . . . this software is emerging out there." *Id.* at 33:48.

5. The District Court's Misunderstanding of the "Concept" or "Idea"

This Election Breach Information is what Defendants repeatedly discussed making public – not any data belonging to Plaintiff, nor even the Chinese Server Data, which has never been in Defendants' possession. Defendant Phillips reiterated that *it was the "idea" or "concept" of American election data being on servers in China* that he wished to reveal, saying, "And by Sunday, we had made a plan to hand this off, *this idea, this concept* off to the FBI, because it was national security." *Id.* at 38:25.

Given this context, Plaintiff has demonstrably misconstrued, misinterpreted, and misstated Defendants' public statements about the data breach Defendants witnessed. And the court inherited that confusion. To the extent Plaintiff's motion and the district court's finding of contempt are both based not on disputed facts but on their own material errors in interpreting Defendants' public statements, and misunderstanding two critical distinctions, the finding of contempt is arbitrary and unreasonable. It is an abuse of discretion and should be purged.

6. Defendants in Good Faith Feared Unnecessary Public Disclosure of Confidential Informants

Moreover, regarding the Chinese Server Data that Defendants did not access and have no legal obligation to assist Plaintiff in securing, Defendants have a good faith, reasonable basis to believe that identifying the third individual in the Dallas hotel room puts him/her at risk for serious harm. Defendants came to the show cause hearing on October 27, 2022, with evidence to corroborate their concerns, but were not permitted to present their evidence to the Court.

On October 6, the court responded to Defendants' counsel's "fear of the safety" of Michael Hasson with the *non sequitur* that "there are no Chinese in here doing anything" and the irrelevant observation that the name of Mr. Hasson "was not a typical -- or even appeared to be a name of a Chinese individual." Doc 30 at

24. Since his outing, Counsel is informed Mr. Hasson appears to have gone into hiding.

Defendants also informed the court they received death threats themselves. Around the time they were told Mr. Hasson had gone into hiding, Defendants hired personal security, who began to accompany them everywhere. Still assuming Defendants had breached anything belonging to Plaintiff, the court dismissed these threats out of hand and appeared to believe them justified:

> MR. AKERS: Both Ms. Engelbrecht and Mr. Phillips have received death threats... She has drones flying over her house.
>
> THE COURT: Well, let me say it like this: If you are looking at somebody else's business, whether it is shown to you by some person that you don't want to tell the name of, or whether it's because you are just nosy... you should expect that... somebody is going to look for you.

Doc 30 at 30, lines 11-17.

And when asked why he did not feel he had authority to give up the name of the third man in the room, Defendant Phillips explained his fears, and alluded to the informant work the unidentified individual has long done at the border.

> THE WITNESS: Well, first of all, it would put his life in danger. Beyond that, because I know that he's a CI, you can't just unmask a person that is a CI. This person -- this particular person, Judge, is -- he would be in such extraordinary danger that --
>
> THE COURT: From?
>
> THE WITNESS: From –

> THE COURT: China?
>
> THE WITNESS: From the cartels. He works on the border. He does all kinds of work.
>
> THE COURT: The cartels on the border, as I understand, are drug dealers.

Doc 47 TR at 103.

All of this gave Defendants reasonable concern that they were about to be accomplices in outing yet another informant, either in open court or through other means. As did the district court's expressed lack of concern about "this man's safety or security":

> THE COURT: I'm not going to enter a protective order to protect anybody and *I'm not concerned about this man's safety or security*. So I'm not going to do it [seal the name]. You are going to do it [disclose the name openly] because you had no right to submit this to me under seal.

Doc 30 TR at 47-48 (emphasis added).

When the district court insisted, during the hearing on October 27, that Defendants also turn over the name of the second confidential informant, Defendants, recalling the district court's unnecessary outing of the first, had a reasonable fear for the safety of that confidential informant. Defendants' fear was only exacerbated when the district court claimed it had the highest security clearance in the land and could not be asked to keep anything confidential:

> THE COURT: . . .And here is the message, lawyers and witnesses or parties: If I am not provided, and counsel is not provided -- you don't have to turn anything over to me confidentially. I have the highest clearance of anybody in this country. *And so you cannot ask me to agree to keep something confidentia*l.

DOC 47 TR at 172: lines 8-15.

C. The Court's Prejudgment of the Defendants' Case

More worrying, the court unnecessarily and unfairly alluding to former President Trump, and thereby heightening the drama, seemed to have made up its mind that Defendants, had "played" their lawyers. The court said it had no confidence in Defendants' work, which is the basis of the non-profit True the Vote and this lawsuit:

> MR. AKERS: I think I'm a better judge of character than that [to be played].
>
> THE COURT: *You would have thought that of the President or a lot of lawyers who have been disbarred or who are being now sanctioned.* I have no reason to believe those weren't good lawyers, but they were played.
>
> MR. AKERS: . . . I'm confident that I have not been played and that the work that they have done is worthy.
>
> THE COURT: The work that who has done?
>
> MR. AKERS: The work that my client True the Vote in order to accomplish election integrity overall –
>
> THE COURT: *I don't really have any confidence in any of these folk who claim they are doing that. We did pretty good until about three or*

> *four years ago*, five or six years ago. The only people that I know of who have done something wrong are people who have been either caught or who have been charged and mistreated. Do errors get made? Yeah. Do people cheat? Perhaps. But all of this fuss and hustle and bustle about the integrity of a process and the way you fix that process is you tear it apart? *That's not integrity. That's destruction.*

DOC 30 TR at 49. The court's comments reflect that it had already made up its mind about the Defendants, their work, and their case. Defendants saw the results in the court's overruling their every objection, and its refusal to let them put on their evidence or witnesses such as the Los Angeles County Assistant DA.

SUMMARY OF ARGUMENT

The court below clearly abused its discretion when it found Catherine Engelbrecht and Gregg Philipps in contempt of court for failing to comply with an immaterial provision of a temporary restraining order that was entered *ex parte* and based on demonstrably flawed reasoning.

REASONS FOR RELIEF AND AUTHORITIES

A. Standards of review

1. Mandamus

"Under the All Writs Act, federal courts 'may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.' 28 U.S.C. § 1651(a)." *In re Gee*, 941 F.3d 153, 157 (5th Cir. 2019).

Included among these writs is the writ of mandamus. Before a court of appeals will issue a writ of mandamus, the applicant must satisfy three conditions:

> First, the party seeking issuance of the writ must have no adequate means to attain the relief he desires – a condition designed to ensure that the writ will not be used as a substitute for the regular appeals process. Second, the petitioner must satisfy his burden of showing that his right to issuance of the writ is clear and indisputable. Third, even if the first two prerequisites have been met, the issuing court, in the exercise of its discretion, must be satisfied that the writ is appropriate under the circumstances.

Id, at 157 (quoting *Cheney v. U.S. Dist. Court for D.C.*, 524 U.S. 367, 380-81 (2004). These conditions ensure that the writ is reserved "for really extraordinary cases." *Id*., at 158. In extraordinary cases, mandamus petitions serve "as useful safety valves for promptly correcting serious errors." *Id*. *See also, Leonard v. Martin*, 38 F.4th 481, 488-89 (5th Cir. 2022).

If the issue raised in the petition is one committed to the discretion of the trial court, "a clear and indisputable right to the issuance of the writ will arise only if the district court has clearly abused its discretion, such that it amounts to a judicial usurpation of power." *In re Gee*, 941 F.3d at 159. "Demonstrating a clear and indisputable right to a writ of mandamus 'requires more than a showing that the district court misinterpreted the law, misapplied it to the facts, or otherwise engaged in an abuse of discretion." *Leonard*, 38 F.4that 489. The petitioner must show "a clear abuse of discretion that produces patently erroneous results" or "exceptional

circumstances amounting to a judicial usurpation of power." The petitioner must show not only that the district court erred, but that it clearly and indisputably erred. *Id*.

2. <u>Contempt</u>

Contempt findings are reviewed for abuse of discretion. Facts are accepted as true unless clearly erroneous, but questions of law concerning the contempt order are reviewed de novo. A factual finding "is clearly erroneous only if, viewing the evidence in light of the record as a whole, [the appellate court] is left with the definite and firm conviction that a mistake has been committed." Whether a contemnor was denied due process of law is a question of law that is reviewed de novo. *Waste Management Inc. v. Kattler*, 776 F.3d 336, 339 (5th Cir. 2015); see also *American Airlines Inc. v. Allied Pilots Assn.*, 228 F.3d 574, 578 (5th Cir. 2000).

Due process requires "that one charged with contempt of court be advised of the charges against him, have a reasonable opportunity to meet them by way of defense or explanation, have the right to be represented by counsel and have a chance to testify and call other witnesses." *Waste Management*, 776 F.3d at 340. "Adequate notice typically takes the form of a show-cause order and a notice of hearing identifying each litigant who might be held in contempt." *Id*.

In *Waste Management*, the Court summarized the requirements for a sufficient contempt order in detail:

> "A party commits contempt when he violates a definite and specific order of the court requiring him to perform or refrain from performing a particular act or acts with knowledge of the court's order." To hold a party in civil contempt, the court must find each violation by clear and convincing evidence. Evidence is clear and convincing if it "produces in the mind of the trier of fact a firm belief … so clear, direct and weighty and convincing as to enable the factfinder to come to a clear conviction without hesitancy, of the truth and precise facts of the case." The contemptuous actions need not be willful so long as the contemnor actually failed to comply with the court's order.

Id., at 341; *American Airlines*, at 581. An alleged contemnor may defend against a *prima facie* showing of contempt by demonstrating a present inability to comply with the court order. *Id.*

B. <u>Application of the standards to the facts</u>

1. <u>What the district court ordered Petitioners to do</u>

On September 12, 2022, after reviewing Konnech's Original Complaint, its Motion for a Temporary Restraining Order (TRO) and Eugene Yu's supporting affidavit, the district court granted Konnech a TRO. Notwithstanding the fact the court had only considered the pleading, the court found that the evidence supported the following findings: (1) Konnech had a substantial likelihood of succeeding on the merits because the Petitioners had allegedly confessed as to having gained unauthorized access to Konnech's protected computers, (2) Konnech was subject to

immediate irreparable harm without the TRO, (3) the harm outweighs any potential harm the Petitioners might have suffered, and (4) the TRO was in the public interest. (DOC 9, pp. 1-2).

The court thereafter entered the following injunctions: (1) Petitioners were not to access or attempt to access Konnech's protected computers; (2) Petitioners were ordered to return all property and data obtained from Konnech's protected computers; (3) Petitioners were enjoined from exploiting any property or data gleaned from Konnech's protected computers; (4) Petitioners were ordered to preserve any information or data obtained from Konnech's protected computers; (5) Petitioners were ordered to identify any and all individuals and entities involved in accessing Konnech's protected computers: (6) Petitioners were ordered to confidentially disclose how, when, and by whom Konnech's protected computers were accessed; and (7) Petitioners were ordered to identify all persons or entities who once had possession, custody, or control or any information or data from Konnech's protected computers. (DOC 9, pp. 2-3).

2. <u>Why the Court ordered the Petitioners detained</u>

During the show-cause hearing on October 27, 2022, Konnech complained that the Petitioners had failed to comply with the fifth, sixth, and seventh directives of the TRO. (DOC 47, pp. 9, 17-19). Petitioners, through counsel, attempted to

introduce an affidavit from Gregg Phillips averring that True The Vote had turned over any information in their possession of FBI special agents, that the amount of information Petitioner Phillips had seen in a Dallas hotel room was too massive to have come from an individual computer, and the material Phillips saw may not even have come from a Konnech protected computer. (DOC 47, pp. 10-12). The district court insisted on receiving the Petitioners' testimony. (DOC 47, pp. 13, 21).

Gregg Phillips testified. (DOC 47, p. 29). Phillips identified one individual that he personally had "access" to material germane to items five through seven of the court's order (DOC 47, p. 31). Phillips testified that he met this individual in a Dallas hotel room in January or February of 2021 (DOC 47, pp 31-32). Phillips testified that what he saw was information that had been downloaded in the past – there was far too much information for a single computer. Neither of the petitioners had possession, custody, or control of that information. (DOC 47, p. 33).

After the meeting, the petitioners turned over what they had to the FBI (DOC 47, p. 34). Phillips testified that he did not know how or when or by whom the information was downloaded but the FBI appeared to deem it significant in light of the volume – more than 350 terabytes had been downloaded over the first quarter of 2021. (DOC 47, pp.35-36). Finally, Petitioner Phillips testified that he was aware of

only two individual agent of the FBI who may have exercised possession, care, custody, and control over the information he saw. (DOC 47, p. 36).

On cross-examination, Phillips admitted one other individual attended the meeting in the Dallas hotel. (DOC 47, p. 39). Phillips refused to identify this individual because Phillips believed him to be an FBI confidential informant (DOC 47, pp. 39-40). Phillips held his position to refuse to identify the individual after the court ordered him to do so. (DOC 47, p. 40). Petitioner Phillips testified that he did not share any of this information with Petitioner Engelbrecht. (DOC 47, p. 52).

Aside from the other individuals in the hotel room and the FBI agents, Phillips had no knowledge of who may have accessed the Konnech-protected computers. When counsel asked Petitioner Phillips whether the data he saw came from a Konnech-protected computer, Phillips said his contacts believed that it came from a server in China. (DOC 47, p. 73).

Petitioner Phillips testified that he had never accessed or attempted to access a Konnech computer himself. (DOC 47, p. 74). During an examination by the court, Phillips continued to refuse to identify the other individual attending the Dallas hotel meeting. (DOC 47, pp. 83-88). When the court asked whether or not Petitioners were going to post personal identification information online, Phillips demurred and advised the court he was alluding to a separate data set, as explained above. The

court declared that it was not interested in separate data sets. (DOC 47, pp. 96-97). The court posed a series of questions that touched upon the toxic culture of internet downloads related to election officials and other public figures. (DOC 47, pp. 97-100). In the end Phillips refused to identify the third individual in the hotel room. (DOC 47, p. 101-103). Phillips confessed if the individual's identity became known his life would be jeopardized by the border drug and smuggling cartels. (DOC 47, p. 43).

Petitioner Catherine Engelbrecht testified. (DOC 47, p. 106). Petitioner Engelbrecht testified that she did not have any personal knowledge with respect to the fifth, six, and seventh directives of the TRO – she received all of what she knew from Petitioner Phillips. (DOC 47, p. 108). Indeed, Petitioner Engelbrecht confessed that she did not have any technical knowledge as to how computer data was conveyed to the FBI. (DOC. 47, p. 114). Engelbrecht testified that she was aware of a program called "BinaryEdge" that could be used to determine the location of a computer server. (DOC 47, pp. 134-135). Information gleaned from these public programs gave Petitioner Engelbrecht that information showing information about American elections ended up on servers in the Republic of China. (DOC 47, p. 139). Petitioner Engelbrecht refused to disclose the identity of the third individual who

attended the Dallas hotel room conference. In fact, because she was not there, she had no direct knowledge. (DOC 47, p. 151).

Notwithstanding Petitioner Engelbrecht's demonstrative lack of knowledge with respect disclosure of information as required by the TRO, the court held her in contempt. (DOC 47, p. 172).

3. The court abused its discretion and that abuse resulted in exceptional circumstances amounting to a judicial usurpation of power.

The district court clearly abused its discretion when it held the Petitioners in contempt of the TRO. The contempt orders rest upon putative violations of the last three directives: to identify any and all individuals and entities involved in **accessing** Konnech's protected computers; to confidentially disclose how, when, and by whom Konnech's protected computers were **accessed**; and to identify all persons or entities who had possession, custody, or control or any information or data from Konnech's protected computers. Violations of these orders turn on the Petitioners' knowledge of unauthorized **access** of Konnech's computers and knowledge of individuals who had possession of data and information gleaned from an unauthorized access. Any analysis of these provisions turns in some part on an understanding of the meaning of "access" under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. The Petitioners had to know who had actually acquired unauthorized access to Konnech's computers. Here, the record does not support the district court's factual

determination that either Catherine Engelbrecht or Gregg Phillips had direct personal knowledge that anyone obtained information from Konnech's protected computers by way of unauthorized access.

"Access" is not defined under the CFAA. "'Exceeds authorized access' is defined as: 'to access a computer with authorization and to use such access to obtain information or alter information in the computer that the accesser is not entitled to obtain or alter." *Dresser-Rand Co. v. Jones*, 957 F. Supp.2d 610, 614 (E.D. PA 2013); 18 U.S.C. § 1030(e)(6). The CFAA governs activity that involves accessing or damaging computers. "Use of the computer is integral to the perpetration of a fraud under the CFAA and not merely incidental. Whatever happens to the data subsequent to being taken from the computers subsequently is not encompassed in the purview of the CFAA." *Id*., at 615. Here, Petitioner Phillips did not execute an unauthorized access into Konnech-protected computers: he saw data on a server, ostensibly located in China, that someone unknown had acquired by accessing a Konnech-protected computer. In fact, the record is bereft of any evidence that Phillips was unaware of anyone who had accessed a Konnech computer.

It has never been established that the computer Mike Hasson evidently accessed belonged to Konnech. At the same time, Konnech has denied its servers

were breached or that it maintained any in China. If that is so, this entire case is moot. That aside, the immediate issue is the arbitrary confinement of two citizens.

To hold a party in civil contempt, the court must find each violation by clear and convincing evidence. Evidence is clear and convincing if it "produces in the mind of the trier of fact a firm belief … so clear, direct and weighty and convincing as to enable the factfinder to come to a clear conviction without hesitancy, of the truth and precise facts of the case." *Waste Management*, *supra*, at 341. Here the clear and direct weight supports a finding that the district court abused its discretion and usurped judicial authority when it found Petitioner Phillips in contempt and ordered him detained.

Petitioner Catherine Engelbrecht's uncontroverted testimony reveals that she had absolutely no knowledge of any unauthorized access to Konnech protected computers. Indeed, she was not event present with Petitioner Phillips in the Dallas hotel room when he was shown on the China data. The finding of contempt against her is a clear abuse of discretion and must be reversed.

CONCLUSION

Petitioners Catherine Engelbrecht and Gregg Phillips pray that this Court grant their petition for writ of mandamus, that the order of contempt be set aside, and that they be released from confinement forthwith.

Respectfully submitted,

GREGOR | WYNNE | ARNEY, PLLC

MICHAEL J. WYNNE
Attorney at Law
Texas State Bar No 0078529
Telephone: (281) 450-7403
mwynne@gwafirm.com

CAMERON POWELL*
Attorney at Law
DC Bar No 459020
Telephone: (832) 390-2644
cpowell@gwafirm.com

JAMES L. TURNER
Of Counsel
Texas State Bar No. 20316950
Telephone: (713) 305-5457
jturner@gwafirm.com

**Pro Hac Vice pending*

ATTORNEYS FOR PETITIONERS

Certificate of Service

I hereby certify that a true and correct copy of the foregoing was served by CM/ECF e-service on November 3, 2022, on the following counsel of record:

Constantine Z. Pamphilis
KASOWITZ BENSON TORRES LLP
Wedge International Tower
1415 Louisiana, Suite 2100
Houston, Texas 77002
dpamphilis@kasowitz.com

ATTORNEYS FOR RESPONDENT

By: /s/ *Michael J. Wynne*
Michael J. Wynne

Certificate of Compliance

This brief complies with the type-volume limitation of FED. R. APP. P. 32(g)(1) and 27(d)(2)(a) in that it contains 7,225 words. It also complies with the typeface requirements of FED. R. APP. P. 32(a)(5) and the type-style requirements of FED. R. APP. P. 32(a)(6) in that it has been prepared in a proportionally spaced typeface using Microsoft Word, Windows 11 in Times New Roman 14 point font.

By: /s/ *Michael J. Wynne*
Michael J. Wynne