UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

KONNECH, INC.,	§	
	§	
Plaintiff,	§	Civil Action No. 4:22-cv-03096
	§	
v.	§	
	§	
TRUE THE VOTE, INC., *et al.,*	§	
	§	
Defendants.	§	

DEFENDANTS' RESPONSE TO PLAINTIFF KONNECH, INC.'S SECOND MOTION TO SHOW CAUSE AND FOR CONTEMPT AGAINST DEFENDANTS RELATED TO THE PRELIMINARY INJUNCTION AND DIRECT ORDERS FROM THE BENCH

The opening paragraph of Plaintiff Konnech, Inc.'s "Motion to Show Cause and for Contempt Against Defendants Related to the Preliminary Injunction and Direct Orders from the Bench" ("Second Show Cause") rehashes the false accusations Konnech has been making from the start, including among other things, that Defendants "admitted" they accessed a computer *belonging to Konnech. See* Second Show Cause at 1 (stating incorrectly that Defendants have any connection to PII "on Konnech's computers").

Plaintiff tries again. It attributes again to Defendants podcast quotations either taken directly out of context or fabricated -- by inserting text within square brackets – and adding words not part of the original quotation. Patching all this together, Konnech cannot help but to inject itself into conversations having nothing to do with it. Konnech seeks again an end around normal discovery. Absent any "emergency" (read immediate and irreparable injury), Plaintiff asks the Court at this premature stage again to bring out the hammer of contempt, recently condemned at this early stage in a civil case by the Court of Appeals. There never was and certainly is not now a likelihood of success on the merits or danger of irreparable harm that would support a preliminary

injunction, much less a finding of contempt. It is time for the Court to examine Plaintiff's patchwork claims more carefully and to vacate the preliminary injunction.

Plaintiff repeatedly says Defendants "admitted" they accessed "Konnech's computers," while at the same time conceding that the only access Defendants have ever spoken or written about was access to a computer server located *in China,* and Plaintiff claims it does not own or have any ownership interest in a server in China.

> Defendants admitted [sic] that, not only were they involved with hacking Konnech's computers, but they know how it was done: "In this case, *the server in China* that was accessed had a pre-loaded password (i.e., 'password') ... (emphasis added)

See Second Show Cause at 8. How Plaintiff can reconcile its claim about Defendants' "hacking [of] Konnech's computers" with its statement Defendants accessed "the server in China" that does not belong to Konnech remains a puzzle. Defendants addressed this in their Mandamus briefing to the Fifth Circuit Court of Appeals (*see* Plf's Mot. Ex. G) and again in their recent Motion to Dissolve the Preliminary Injunction, citing both the language of the actual podcast statements forming Plaintiff's only basis for a Computer Fraud and Abuse Act (CFAA) claim and the unrebutted testimony of Defendants. In sum:

1. Plaintiff has never stated a proper claim that any of its own computers were accessed, including by properly specifying an actual computer and its IP address, or showing Defendants "admitted" to hacking a computer Konnech actually owns.
2. The Court of Appeals rightly concluded that Plaintiff had thus established no "emergency" justifying injunctive relief and short-circuiting traditional discovery. Moreover, given that Plaintiff's demand for a TRO and preliminary injunction were founded on the immediacy of an election that took place well over a month ago, the supposed danger of "irreparable

harm" justifying any extraordinary and one-sided discovery is even less now than it ever was.

3. Plaintiff has failed to show that Defendants ever possessed or threatened to disclose any data taken from Konnech.[1] *See* Defendants' Mandamus from the United States District Court for the Southern District of Texas, hereafter "Mandamus Petition").
4. Plaintiff's own pleadings consistently concede that whenever Defendants spoke of "access", they were referring to a server in China that Plaintiff adamantly says it does not own, confirmed by the only evidence in the record, unrebutted testimony from Defendants Engelbrecht and Phillips at the October 27, 2022, contempt hearing.

Regarding the central issue, Plaintiff unaccountably claims "Defendants have presented no evidence and cited no authority to warrant their refusal to disclose the individual's identity." Second Show Cause at 15. This is nonsense. Defendants have explained, many times now, that alleged access of a server in China, whose ownership Konnech has to this day not claimed, fails to implicate any interest whatsoever of any "Konnech computer" in the United States. And because this Court's order requires Defendants only to disclose the identities of persons who "accessed" a "Konnech computer," Defendants' refusal to discuss access of a computer in China is, to put it mildly, "warranted".

Plaintiff adds new speculation in its recent Response to Defendants' Motion to Dissolve the Preliminary Injunction. There, Plaintiff implies that because a server — in China or elsewhere — contained Konnech data and domain names, that server *must have been Konnech's*. But that

[1] Plaintiff makes much of representations from prior Defendants' counsel, in a September 15 letter, which averred "that an individual hacker 'turned over to True the Vote a hard drive device containing' the data stolen from Konnech, which Defendants then turned over to the FBI." Plf's Mot. at 4. The simple answer to this that prior counsel was mistaken, and his representation is not evidence. It is also directly refuted by unrebutted testimony from the only people the Court has forced to testify, or provide discovery, in this case: Defendants Engelbrecht and Phillips themselves.

conclusion is not warranted. There are other possibilities neither Plaintiff nor the Court has ruled out, including that Konnech's data got put on a server in China, one not owned by Plaintiff, through no action of Defendants. Had Konnech already been hacked and had its data moved to China? So long as that remains a possibility, and one that might be explored in full discovery, the Court may make no factual finding that Defendants "admitted" to hacking a Konnech computer. Plaintiff also implies, without evidence, that Defendants lied about the computer *being* in China — but this too is a factual question that has yet to be resolved in any hearing or pleading in this case.

Plaintiff's short-circuiting discovery and insulating its own witnesses from questioning on exactly these points, has reached a point of absurdity. It is time to end this charade and move on to discovery, where Plaintiff will need to try to show that its wordsmithing of a CFAA claim stands up to the barest evidence of what really happened.

In any event, the Fifth Circuit has already rejected what Plaintiff seeks here. The Court of Appeals in *Phillips*, No. 22-20578, 2022 WL 17175826, at *1 (5th Cir. Nov. 22, 2022) (hereafter "*Phillips I*"), ruling on Defendants' Mandamus Petition, stated "the district court's TRO was invalid because it disregarded the order of operations imposed by the Federal Rules." The Court of Appeals unmistakably disfavored Plaintiff's efforts to achieve premature and one-sided discovery, let alone contempt:

> Such a demand makes perfect sense when made by a plaintiff in discovery. But the record does not reveal what sort of emergency justified . . . that information *before* the parties could file Rule 12 motions, *before* the defendants could file an answer, *before* the parties could file their initial disclosures, or *before* discovery could begin let alone conclude in the ordinary course. *Id.* (emphases in original).

With neither disclosures nor discovery yet begun, it is difficult to imagine how the Court of Appeals could have spoken any more dispositively to the *demands* of Plaintiff's *Second* Motion to Show Cause.

The Fifth Circuit went on to hold that "[i]t necessarily follows that any contempt order premised on violations of the [invalid] TRO was "bottomed irrevocably on a mistake of law" (citation omitted). It also necessarily follows that the preliminary injunction, founded on an invalid TRO, based on the same failure of Konnech to state a claim with any likelihood of success, and based on the same failure of Konnech to plausibly allege any "irreparable injury", is without force and must be dissolved. The Fifth Circuit has already disposed of the required pillars of Plaintiff's quest for an injunction and a finding of contempt by noting the lack of any "emergency," which is a comment at least at this juncture on Plaintiff's likelihood of success and its made-up claims of irreparable harm. In the alternative, because the preliminary injunction, (1) like the TRO, puts the cart before the horse, and amounts to a premature discovery order, and (2) was premised on claims of urgency related to an election now already past, the Court should dissolve the preliminary injunction and deny Plaintiff's Second Show Cause. Should the Fifth Circuit's pronouncement be insufficient, Defendants present the following further detail.

I. Introduction: Plaintiff Has Confused the Court Into Thinking Computers Owned by Konnech Are at Issue Here.

Plaintiff's pleadings, which attempt to justify an emergency CFAA claim with misleadingly edited content from web pages and podcast transcripts, are consistent about one thing: the parties are talking about computers, but they're not talking about the same computer.

Plaintiff's Complaint, Motion for TRO, and all its other pleadings allege imagined violations of the "***Konnech computer***". We know the Konnech computer has never been breached, because the Konnech computer, Konnech assured visitors to its website, is secure. There is no

evidence any Konnech computer has ever been hacked, by anybody, anywhere.[2] The Konnech computer is owned by Konnech. The Konnech computer is physically located in the United States.

Meanwhile, the Chinese Server that *Defendants* are talking about in the same podcasts is not in the U.S. (Defendants aimed to confirm this in the October 27 and 31 show-cause hearings with testimony from the Los Angeles County DA's Office, among other means). Defendants' unrebutted testimony and public statements cited in Plaintiff's own pleadings consistently feature a "server," as a type of computer is called, located in *China*. This server was *not* secure. This server was *not* owned by Konnech. This server was *easily accessed* by third parties. Defendants have consistently said the server alluded to in the podcasts was in China, as did Plaintiff, *see* Compl. ¶ ¶ 46-48. *There is no evidence in the record indicating otherwise*.

If the never-accessed and never-identified Konnech Computer and the Accessed Chinese Server look like two different computers, that's because they are. Plaintiff's invocation of CFAA penalties and fines thus fails to state a claim. The Court must take notice that the same podcast statements made by or attributed to Defendant Gregg Phillips, on which Plaintiff solely relies, show he has consistently said he viewed data from a computer *in China*. (Konnech implies that the identification of a computer in China is false; if so, it's an unresolved factual question meriting discovery).

In pleading after pleading, Plaintiff has studiously avoided facing this conundrum, one that is not only fatal to its claims of computer access but carries with it catastrophic implications for

[2] Konnech claims that its inability to prove anyone accessed its computer does not mean it was not accessed; that is probably false, yet showing as much would require that this matter return to the normal process of discovery and expert testimony to explain that Konnech would have server logs, in its possession, showing access of its own computer, with a particular IP address, by another computer, with an identifiable IP address. Moreover, the fact that the domain names belonging to Plaintiff and its customers were *also* hosted on the very same Chinese server would have been impossible for any competent technology company to miss.

Konnech.[3] Plaintiff has offered neither contrary evidence nor a rebuttal rooted in Defendants' actual statements. Plaintiff just keeps pointing to its misleading massaging of transcripts from Defendants' podcasts, which confirm that Plaintiff's case rests entirely on conjectural square brackets and tortured paraphrasing to allege in conclusory language "access" to a "Konnech computer" in the United States. The Fifth Circuit got it right.

II. Plaintiff Cannot State a CFAA Violation, Let Alone Plead Sufficient Facts Justifying a Preliminary Injunction.

A "plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Nat. Res. Def. Council, Inc*., 555 U.S. 7, 20 (2008).

Plaintiff staked its claim to federal jurisdiction (1) on implausible conclusions – e.g., that all three Defendants somehow "accessed" a "Konnech computer" – and (2) on implausible representations of Defendants' public statements that fail to state a claim in the first place. Plaintiff certainly cannot meet the much higher standard required to obtain a TRO or a preliminary injunction.

---

[3] The reason Plaintiff must ignore the Chinese server is that Plaintiff cannot or does not wish to explain how Defendants could have found data, originating from Plaintiff, on a server in China.

Both possibilities, the only possibilities, are very very bad for Konnech. One possibility is that Konnech's computers in the U.S. were hacked by a third-party, who transferred the data to a server in China, where it was then accessed by Michael Hasson before he showed some of the data to Defendant Phillips in that Dallas hotel room. With its now-dismissed indictment, Plaintiff's customer Los Angeles County has already shown just how unhappy this possibility would make Plaintiff's customers. Plaintiff cannot utter this possibility aloud.

The second of only two possibilities is that Plaintiff itself, or a vendor, maintained a server in China and hosted Konnech's domain names and customer PII there. Perhaps Konnech was not even aware of it; in any event, this possibility would actually make Plaintiff's customers even more unhappy. Plaintiff dares not put this possibility into writing.

Plaintiffs' solution seems to be to imply without saying so that Defendants are lying about the Chinese server and must have hacked an unidentified computer that *did* belong to Plaintiff, and, separately, Plaintiff's domain name servers, all without Plaintiff noticing, and put the data and domain names on the Chinese server.

The Court should itself review the podcasts. The Court is obliged to review all such documents incorporated into the complaint by reference, or documents integral to the claim, as well as items subject to judicial notice and matters of public record. *See Funk v. Stryker Corp.*, 631 F.3d 777, 783 (5th Cir. 2011). If the Court wishes to entertain quotations from public transcripts to form the basis of emergency *ex parte* hearings and orders of contempt, the Court should make a reasonable, independent inquiry as to whether Plaintiff's representations of Defendants' statements amount to conclusory and unwarranted inferences or even, as here, outright misrepresentations. "The district court abuses its discretion when its ruling is based on . . . a clearly erroneous assessment of the evidence." *Funk*, 631 F.3d at 783.

Almost the entirety of the Complaint and pleadings requesting injunctive relief are premature efforts to obtain one-sided discovery. They amount to (1) Plaintiff's battery of tendentious, disparaging, and extraneous allegations designed to inflame the reader, and (2) Plaintiff's defamation claims. Plaintiff's CFAA claims are set out in Paragraphs 7[4], 40-42, and 46-48 of the Complaint. Plaintiff seeks to engage in one-sided discovery, with the threat of contempt available, by virtue of selected quotes Plaintiff has strung together from *Defendants' podcast statements about a server in China*. Strikingly, in Paragraphs 46-48 of the Complaint, Plaintiff *admits* that Defendants were always talking about a server in China:

> 46. . . . Defendants have falsely accused Konnech of storing sensitive and personal data . . . on 1.8 million U.S. poll workers *on servers in China*, and otherwise running their election logistics application through *Chinese servers*." . . . .
>
> 47. . . Defendant Phillips falsely claimed that Konnech "left a database open that had the personal identifying information of over a million Americans living *on an open server in China*."

[4] Paragraph 7 contains the most conclusory of the allegations, alleging Defendant Phillips "successfully hacked into Konnech's servers and unlawfully downloaded its data" and that Defendants "repeatedly declared their intent to release the information they stole from Konnech's servers." Because Plaintiff is slightly more specific, if no less conclusory and implausible, in Paragraphs 40-42, we focus on those paragraphs.

> 48. . . . Defendant Phillips falsely claimed that Konnech's election software "apps *were running from China, the database is running in China. It's on the Chinese internet, meaning the Chinese own it*."
>
> (Emphases added.)

So it's inexplicable that, though Phillips never mentioned Konnech in the quoted podcast segments, Konnech, in Paragraphs 40-42, tries to insert itself into a stated CFAA claim via two misleading methods: (1) Konnech ends Phillips's quoted content and then inserts the word "Konnech" in place of the Chinese server or data to which Phillips is plainly referring, and (2) Konnech keeps the quotation marks but inserts "[Konnech]" in square brackets meant to suggest to a reasonable reader that "Konnech" is plausibly what Phillips was speaking about. Both amount to frivolous exercises.

We can first see the latter misleading method hard at work in Paragraph 40, the first of the three paragraphs purporting to make out Plaintiff's CFAA claim. That paragraph refers to the Prophets and Patriots podcast:

> Indeed, Defendant Phillips admitted on that podcast[5] that "[w]e took [Konnech's data] directly" and that Defendant True the Vote plans to publicly "release all of [Konnech's] data" through "drops" to subscribers of Defendants' website.

Plaintiff provided no transcripts (or even a link) from the "Prophets" podcast, likely because doing so would have exposed the fact that under no honest use of language could one say Phillips "admitted" to taking "Konnech's data". First, the Court could readily confirm that what Phillips said, disregarding Plaintiff's disingenuous square brackets (and in a throw-away aside), was "We took *it* directly" -- and it's not at all clear from the context what he meant by "it" or even "took". But one thing is quite clear: he's talking about data on a server in China. The "We took it directly" language is bracketed on both sides by *China*:

[5] *See* https://rumble.com/v1h1pj9-rumble-only-prophets-and-patriots-episode-20-with-gregg-phillips-and-steve-.html

> . . . but what if your data was all being ***filtered through China***? And what happened was, we're not asking anyone to believe us. We took it directly. That was on a Friday night.
>
> My guys invited me to Dallas on a Friday night. We went, met at a hotel room, towels under the doors. It was pretty weird. I mean, it was like some kind of a James Bond kind of thing or some sort of weirdness like that. And they proceeded to show me everything. ***They showed me the database, they showed me where it lived. It lives on the main unicorn backbone in China, which is the main Internet in China.***
> *See* "Prophets"[6] at 41:47 to 42:32 (emphases added).

Second, the Court may confirm that only much later in the "Prophets" podcast (at 51:13) did Phillips say, "we're gonna release *all of our research*" and he was unmistakably referring to *his* research and data – not Konnech's: "we're going to release all of ***our research***. We're going to release ***all of our data***." (Emphases added). This "data" included *video* unrelated to Konnech's PII data: "We still haven't figured out exactly how to release all the video." *Id*. at 51:17. Konnech, its computers, and its PII data are nowhere in evidence. Plaintiff has simply willed itself into a conversation that doesn't involve it.

In Paragraph 41, Plaintiff grossly misrepresents the contents of the "Midterms" podcast:

> 41. Defendant Phillips repeated these claims on an August 30, 2022 podcast titled, "Here's How They'll Try to Steal the Midterms,"[7] where Phillips described, once again, traveling to Dallas, Texas to meet his so-called "analysts," where they *"*plugged one of their computers into the television*"* and began *"*scrolling through millions and millions of records about Americans*,"* all of which he claims to have obtained by gaining unauthorized access to Konnech's protected computers. Defendant Phillips also described how he "immediately drove down to Houston" and got Defendant Engelbrecht "to come over and meet [him]" that next morning, where they came up with a plan to file a complaint with the FBI and turn over the data they stole. (Emphases added)

To patch together Paragraph 41, Plaintiff must forage across the "Midterms" transcript, piecing together language out of context to suit its narrative. Plaintiff grabs the language about those in the Dallas hotel room who "plugged one of their computers" from a conversation at 35:29

[6] *See* https://rumble.com/v1h1pj9-rumble-only-prophets-and-patriots-episode-20-with-gregg-phillips-and-steve-.html
[7] *See* https://rumble.com/v1hz1jr-heres-how-theyll-try-to-steal-the-midterms-gregg-phillips-interview.html.

in the podcast. But Phillips' statement makes clear that the accessed server was in China, and at 34:54 he explains how he knew it was in China:

> [The website Binary Edge] tells you where it lives, where does the server live, and you could actually track it down and you track it down to China. On the main Unicom backbone in China, it was almost impossible for me to believe.

For the language about "scrolling through millions and millions of records," Plaintiff must leap to a different part of the transcript, at 36:57. But once again, the full quote shows Phillips was clear about the server's being in China, and "Konnech's computers" are nowhere in sight:

> [T]he other thing that your fearless listeners need to understand is that ***by Chinese law, if something comes onto the Chinese backbone, in other words, it's in the Chinese Internet***, that means the CCP owns it. What I'm telling you is that that night in mid-January of 2021, I personally witnessed the scrolling through of millions and millions of records about Americans. We later found out that that was attached directly to the [Chinese] social scoring system . . .
>
> *See* "Midterms" podcast, 36:32 to 37:08 (emphases added).

Plaintiff tortures language and logic once again in Paragraph 42 of its Complaint:

> 42. Likewise, on a September 2, 2022 podcast hosted by Defendant Phillips called "Patriot Games"[8] . . . Defendant Engelbrecht . . . confessed to how Defendants conspired to *unlawfully access* ***Konnech's*** *protected computers*, and how she and True the Vote "pulled in [Defendant Phillip's] team, and asked them to take a deeper dive" around the security of ***Konnech's*** *software*. Defendant Phillips told The Pit attendees that they accessed ***Konnech's*** alleged ***Chinese server*** by using a password after finding vulnerabilities in the server.

(Emphases added). The Court would hear in the "Patriot Games" audio of the actual podcast no such "confession" of unlawful access. The Court would not even hear the word "Konnech." But even if Defendant Engelbrecht, who no one alleges was even present, could have somehow "confessed" to accessing a server, *Plaintiff's Paragraph 42 itself* makes clear that the server each Defendant was referring to was an insecure "Chinese server", which is fatal to Plaintiff's allegation anyone gained access to one of its secure, U.S.-based computers. Plaintiff cannot credibly base a

[8] *See* https://podcasts.apple.com/us/podcast/gamechanger/id1634272318?i=1000578182010.

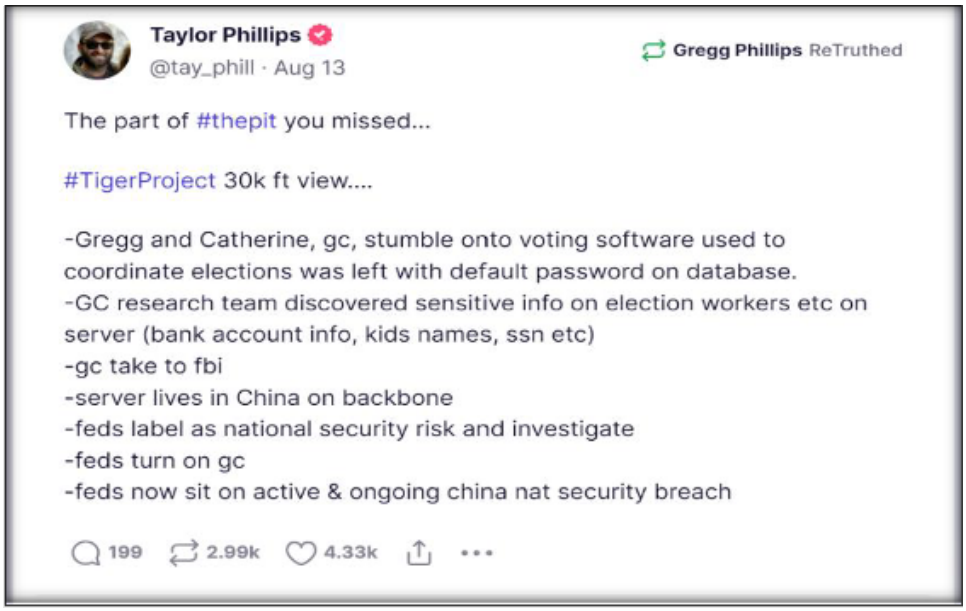
claim of access solely on statements by Defendants but ignore the inconvenient and inconsistent but outcome determinative parts of those statements.

Three disingenuous paragraphs, each misrepresenting the contents of a different podcast, are the extent of Plaintiff's CFAA claim. It has become clear that Plaintiff does not want to acknowledge ownership of the only server (the Chinese Server) for which there is any alleged "evidence" of access. Plaintiff's reluctance could be due to the fact that Konnech did not own a server in China – though it still very much wants entrée to the CFAA's stiff penalties. Or Konnech did own the server in China, but knows its customers, to say nothing of regulators, would be alarmed if it said so. Konnech has compromised by arguing that when Defendants clearly speak of an insecure Chinese server that Konnech does not claim to own, they are lying, and really are referring to an unidentified U.S. server that Konnech does own. This misshapen compromise fails to state a claim under the CFAA and certainly fails to meet the even higher burden of showing a likelihood of success on the merits or a danger of irreparable harm. To the extent Plaintiff implies Defendants are lying about the server being in China, that is a disputed factual question.

However, the Court has mistakenly accepted Plaintiff's misrepresentations. The Court in its Memorandum Opinion and Order on Motion for a Preliminary Injunction made a telling error when it cited a third party's social media post and stated, as grounds for Defendants' supposed "access" of "Konnech's computer," that "*[t]he defendants* describe their acquisition of [Konnech's] data as follows":

> Gregg and Catherine, gc, stumble onto voting software used to coordinate elections was left with default password or database. GC research team discovered sensitive information on election workers, etc. on server (bank account info, kids' names, ssn etc-gc takes to fbi . . .

(Emphasis added). But this text does not come from Defendants. As Paragraph 24 of the Complaint itself makes clear, the text was written by a third party. The Complaint even featured the original image of the social media post by one Taylor Phillips:



This hearsay text doesn't even indicate that a computer *owned by Konnech* was accessed by Defendants. Notwithstanding the post clearly saying the "server lives in China," the Court seems to have assumed the server was Konnech's. And on October 27, the Court questioned Ms. Engelbrecht about the social media post under the mistaken assumption that she had written it.

THE COURT: ***Does this sound familiar to you***: Gregg and Catherine, GC -- that's you, Gregg and Catherine -- stumbled onto voting software used to corroborate elections. Was left with default password.

* * *

THE WITNESS: No, sir. It ships with the password. I think that is what it's referring to.

THE COURT: No. I'm asking ***you*** what ***you're*** referring to.

It says here: You were left with -- you used to coordinate the elections, was left with default password of database.

What are ***you*** talking about?

> * * *
>
> THE COURT: But ***you're the one talking about it***.
>
> * * *
>
> THE COURT: Well, ***you*** said ***you stumbled*** onto voting software used to coordinate elections.

See Oct. 27 TR at 94-99 (emphases added).

In short, it is time to end the farce of Plaintiff's claim that anyone has "admitted" accessing any of its computers, let alone taken anything from them.

A. Plaintiff Failed to State a Claim Under the CFAA.

E*ven assuming Plaintiff had claimed Defendants' access of a computer owned by Konnech,* which it did not do, Plaintiff's Complaint fails to identify which provision of the CFAA Defendants would have violated. This alone should be fatal to any CFAA claim, let alone to any claim of likelihood of success on the merits to support a preliminary injunction.

Likely because it can show no actual access of any of its computers, Plaintiff's Complaint fails to cite any particular section of the CFAA it believes was violated by Defendants' podcast transcripts, including but not limited to Section 1030(a)(1)[9], Sections 1030(a)(2)(A) (referring to various "financial institution", "card issuer", or consumer reporting agency records) or (B) (referring to "information from any department or agency of the United States"), Section 1030(a)(3) (referring to "nonpublic computer[s] of a department or agency of the United States"), Section 1030(a)(5) (referring to malware), Section 1030(a)(6) (referring to password-trafficking on computers "used by or for the Government of the United States"), or Section 1030(a)(7) (referring to extortion). One might speculate that Plaintiff intended to plead a cause of action under

[9] "(a) Whoever - (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information ***that has been determined by the United States Government pursuant to an Executive order or statute to require protection*** against unauthorized disclosure for reasons of national defense or foreign relations"

Section 1030(a)(2)(C), which relates to "intentional" access by which one acquires "information from any protected computer", but whether Defendant Phillips, the only person in the room during any arguable "access", did so "intentionally" to a computer *owned by Konnech* is a question of fact and law that neither Plaintiff nor the Court has addressed.

In addition, Plaintiff's Complaint, in Paragraphs 85 and 99, mentions the $5,000.00 threshold of Section 1030(a)(4), suggesting that perhaps Plaintiff intended to claim a violation of that section, which applies to whoever "knowingly *and with intent to defraud*, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." (Emphasis added). But Plaintiff failed to plead any "intent to defraud", and even if it had, such a pleading would have warranted a fact-based inquiry that would have required discovery or testimony in the ordinary course of a civil lawsuit. In short, it is impossible to conclude that Plaintiff even stated a claim under the CFAA, let alone that it met the higher standards necessary for a preliminary injunction.

III. Because Plaintiff's Claims of "Access" Implicated Novel Legal Conclusions Not Yet Addressed, and Does Not State a Claim in Any Event, the Preliminary Injunction was Unwarranted.

Plaintiff's allegations include the observation that Defendants stated the Chinese Server was "unsecured" and "was left with default password on [the] database...." Compl. ¶ 24. But even if we assume *arguendo* we are talking about a U.S.-based computer owned by Konnech, whether such access was "without authorization," or "exceeds" what is authorized, is a complex legal and factual question that the Court did not address. Moreover, whether a party can be held to access "without authorization" a computer that auto-populates with its own password, in some as-yet

factually undeveloped fashion,[9] is a novel question of law Plaintiff glosses over. In *hiQ Labs, Inc. v. LinkedIn Corp*., 31 F.4th 1180 (9th Cir. 2022), the Ninth Circuit engaged in a lengthy analysis of the statutory language, legislative history, the Supreme Court's opinion in *Van Buren v. United States*, __ U.S. ___, 141 S. Ct. 1648 (2021), and the plain meanings of the terms employed to find that the party accused of access there, hiQ Labs, had "raised a serious question" of law as to whether, "where access is open to the general public," as arguably was the case here, "the CFAA 'without authorization' concept is inapplicable." *hiQ Labs*, 31 F.4th at 1195.

In this case, Plaintiff acknowledges that the accessed server in China featured a pre-loaded password that did not even require anyone to type in a password. Plaintiff has argued that use of the password – and whether "use" is even the correct concept is unknowable without *discovery* from the person who actually accessed the Chinese server – was "unauthorized," but Plaintiff can offer no legal support. The Court here seems to have assumed that such access of the Chinese server was "unauthorized", without considering whether the existence of a default password on even a *Konnech-owned* server rendered access the equivalent of, say, password sharing among friends and family, which would inadvertently "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012).

A. Because Plaintiff's Claims Could Not Survive Scrutiny Under the Lower Standard of a Motion to Dismiss, It Cannot Show Any Likelihood of Success on the Merits for a Preliminary Injunction

The Supreme Court has warned that "the tenet that a court must accept as true [on a motion to dismiss] all of the allegations contained in a complaint is inapplicable to legal conclusions. Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Ashcroft*, 556 U.S. at 678–79 (2009). Here, Plaintiff's claims regarding "access" are both (1) conclusory in nature – as even a cursory examination of its cited statements confirms

– and (2) conclusions of law masquerading as factual allegations (e.g., "Defendants *admit* access"). No preliminary injunction should issue, or remain, under such a pleading.

The second problem with Plaintiff's claims regarding "access" under *Ashcroft* is that "only a complaint that states a plausible claim for relief survives a motion to dismiss. Determining whether a complaint states a *plausible* claim for relief will . . . be a context-specific task that *requires the reviewing court to draw on its judicial experience and common sense*." *Ashcroft*, 556 U.S. at 678–79, (emphasis added; citations omitted). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft*, 556 U.S. at 678 (2009). "Nor do we accept conclusory allegations [or] unwarranted deductions." *Southland Sec. Corp. v. INSpire Ins. Sols., Inc.*, 365 F.3d 353, 361 (5th Cir. 2004). As we have shown above and show further below, Plaintiff's patchwork argument of literary interpretation in place of factual allegations has never been plausible enough to survive the lower standard of a motion to dismiss, let alone justify a preliminary injunction.

B. Plaintiff Has Failed to Claim the Only "Accessed" Computer Was Its Own.

In lieu of its *273-page* Response to the Plaintiff's Mandamus Petition, *see* Plf's Ex. G, and all of its pleadings here, Plaintiff has had at hand a short and simple means to state a claim of CFAA "access" here: Plaintiff could have claimed ownership of the IP address Defendants provided, in their Complaint, for the accessed server based in China. "That is indeed our computer," Plaintiff could have said. But Plaintiff did not, and still has not.

Instead, Plaintiff continues to fall back on its shamelessly misleading use of square brackets to suggest that when Defendants said "computer", in statements scattered across the Internet, they can only have meant "[Konnech] computer," and that when Defendants said "the data" or "it" they were, by some means inaudible to the average listener, talking about "[Konnech] data."

IV. Plaintiff Failed to Show Imminent Harm to Any Computer, While Defendants Have Already Been Gravely Harmed by Plaintiff's Implausible Claims.

Plaintiff's Complaint and Motion for TRO are breathless in their allegations that Plaintiff required urgent, even *ex parte*, relief for some unidentified U.S-based computer, lest Defendants seek to harm that unidentified computer or disclose data stored on it. But where Plaintiff's sole allegation was based not on evidence but a circuitous argument that when Defendants spoke about a computer in China, not Konnech's, they were somehow still talking about a U.S-based computer owned by Konnech, the Court could not have found and cannot now affirm any likelihood of imminent harm to a "Konnech computer".

In its December 5 Petition for Rehearing En Banc, Plaintiff repeats its tired claim that Defendants "admitted" to accessing a Konnech computer, and then makes clear that the TRO was based in part on the emergency of the upcoming election – a cry of wolf that died with a whimper during the election over a month ago. The TRO, Plaintiff explains in its Petition for Rehearing En Banc:

> expressly explained that "emergency conditions exist" because Konnech "will suffer immediate irreparable harm absent the issuance of a TRO" for the reasons explained supra pages 1-2. (App 40-42).
>
> Importantly, the TRO was issued mere weeks before the ***2022 midterm elections***, for which Respondent had several contracts with voting districts to supply its poll worker logistic services for the election and, as such, it ***was vital*** that Respondent obtain the TRO to protect the PII entrusted to it before the election.
>
> Specifically, it ***was vital*** to obtain the identities of the persons involved so that they too could be restrained before causing further irreparable harm before the midterms. (See App 190-205). It ***was also necessary*** to know how Konnech's computers were accessed so that any alleged security flaw could be remedied before the election. (Id.) And moreover, it ***was necessary*** to immediately know who all possessed the PII so that they could be restrained before publicly releasing it. (Id.) As the District Court further explained, "the TRO would in fact benefit the ***public's expectation of integrity in the U.S. election process***." (App 40-42).
> (Emphases added)

On Page 21, Plaintiff adds, "If Konnech were forced to wait to obtain a TRO until after discovery had begun, much less completed in its ordinary course, all damage it sought to prevent before the 2022 midterm elections would have occurred." Well, except we are now comfortably past the midterm elections and no damage has occurred. No damage *could* have occurred because Defendants never accessed a computer belonging to Konnech and Defendants never had or threatened to release any data belonging to Konnech. The Court, too, in its order issuing the preliminary injunction (p. 7), placed substantial weight on Konnech's status as an elections software provider and the then-upcoming election as grounds for the injunction:

> The evidence shows that Konnech provides governmental entities in the United States with an ***election logistics software***, called Poll Chief, that is used by the governmental entities to recruit, train and schedule poll workers, including other polling duties. On or about August 13, 2022, the defendants announced that they were engaged in an attack against Konnech, claiming that Konnech and its President, Eugene Yu, were Chinese operatives working for the Chinese Communist Party to ***interfere with elections in the United States***.
>
> [Defendants' release of data], in the Court's opinion, ***would destroy trust in the governmental entities by the public and, trust between the governmental entities and Konnech***. . . . ***Therefore***, the Court is of the view that Konnech has demonstrated facts that support the issuance of a preliminary injunction. (Emphases added.)

The facts and equities are now entirely different from what they were prior to the issuance of the TRO and the preliminary injunction alike. Even if "it was vital" once upon a time for Plaintiff's emergency relief, that is no longer the case.

As Plaintiff's use of "was" in the language cited above makes clear, it *is* no longer "vital" that "Respondent obtain the TRO to protect the PII entrusted to it before the election." It *is* no longer "necessary" to know how Konnech's computers were supposedly accessed "before the election." It *is* no longer the case that the TRO could "benefit the public's expectation of integrity in the U.S. election process." The facts have changed.

At the same time, the individual Defendants, Engelbrecht and Phillips, have already been harmed by the TRO and injunction below. They *were in reality* subjected to injunctions that were a physical impossibility with which to comply, together with incalculable cost and stress. They *were in real life* held in contempt and confined in jail for a week under an invalid order of contempt, causing immeasurable damage to their reputations. The balance of harms here thus tilts in favor of Defendants, and the harms are no longer even speculative. The harm to Defendants was real and has already been visited upon them.

V. The Suggestion a Spreadsheet File Title Mentioning "PII" Somehow Implicates Konnech is Frivolous.

Plaintiff appears never to have met a series of unfounded assumptions it could not miscast as "evidence" or "admissions". The latest instance in which Plaintiff has decided that something must refer to Konnech when it has absolutely no basis for thinking so comes courtesy of its claim that an ODS (OpenDocument Spreadsheet) file name found among Defendants' 20 months of texts with the FBI must somehow involve Konnech. "*There is evidence*," Plaintiff begins, already misstating the facts:

> to suggest that Defendants also violated Section 4 of the Preliminary Injunction which required them to return all Konnech data in their possession to Konnech. On October 28, Defendants filed an affidavit signed by Defendant Engelbrecht which attached text messages of her alleged communications with the FBI about Konnech. Embedded in those text messages is a spreadsheet titled "Sort by State PII filter SSN Dupes DLN," which, considering that this file is contained in text messages between Defendants and purported FBI agents with whom Defendants were in contact concerning Konnech, *the data therein may include stolen Konnech data*. Therefore, given Defendants' testimony at the show cause hearing that they never had such PII, Defendants *may be in further contempt* of the Preliminary Injunction by refusing to return the data contained in this file to Konnech, as required by Section 4 of the Preliminary Injunction.

Plf's New Mot. to Show Cause at 4 (emphases added).

The illogical leap here comes when Plaintiff assumes the only thing Defendants ever discussed with the FBI was Konnech, and therefore the file must relate to Konnech, and therefore

that it "may" include stolen data. This is all nonsense, repeated on the Motion's page 9: "given that it [the screenshot] was submitted as evidence in connection with this matter, *it appears to relate to Konnech*." (Emphasis added). No such thing "appears". While it is surely disappointing to Plaintiff to hear it, Defendants spoke with the FBI, over a period of about 20 months, about many matters other than Konnech. The number of assumptions Konnech has made here is best revealed by reciting the inconvenient facts – as Defendants' counsel communicated them to Plaintiff, in an email, on December 5, 2022 – hours before Plaintiff inserted its baseless assumptions into its Motion for Show Cause:

> Regarding the .ODS file you reference (if it was ever an actual ODS file, see below), the following is our understanding:
>
> 1. The file was not created by our clients, or anyone associated with them.
> 2. The file came from a suspicious source, via Telegram, who remained anonymous and made threats against Gregg Phillips if he did not do something with the file. (It's unclear as of this writing whether the phrasing was "do something with" or "open" the file).
> 3. The broader context of the file's transmission to our clients gave them no reason to believe it had anything to do with Konnech. Of course, Konnech also lacks any plausible basis to believe that the document had anything to do with Konnech, including with PII belonging to it or its customers.
> 4. Our clients reported the threats and the existence of the file to the FBI, and informed the FBI that they had not opened the file.
> 5. Our clients have no knowledge as to whether the FBI possesses the document.
> 6. Our clients never attempted to open the document, in part because they feared it could contain malware.
> 7. Our clients closed down the Telegram account through which the file came. It does not appear they have any access to an ODS file. When they attempt to forward it, all they see is a PNG image file.

Defendants Engelbrecht and Phillips confirm these statements in their affidavits. *See* Exhibits A and B. There is nothing to Plaintiff's assumptions – concerning a file that bears no indicia it has anything to do with Konnech and that no longer exists in any event – that requires the resources of a federal court to resolve by once again short-circuiting standard discovery procedures and issuing contempt findings.

Conclusion

The now-dissolved TRO, which has been replaced by the preliminary injunction, ordered Defendants (v) to "identify each individual involved in accessing ***Konnech's protected computers***" (vi) to "disclose" by whom "***Konnech's protected computers***" were accessed, and (vii) to "disclose" who retains possession of any data accessed from "***Konnech's protected computers"***. Defendants have answered truthfully that they are not in a position to respond with direct evidence to any of these interrogatives. But there remains a fundamental issue. There is no credible allegation anyone "accessed" a "***Konnech computer****"* or for that matter even a computer located in the territorial United States.

The TRO and subsequent preliminary injunction were entered after the Court (1) took at face value alarmist allegations in a flawed Complaint; and (2) accepted Plaintiff's invitation to use an emergency procedural vehicle poorly suited to this nuanced scenario. There is no reason to go further along this course. If anything, regular discovery may be appropriate.

Wherefore, Defendants ask the Court to deny Plaintiff's Second Motion for Order to Show Cause to grant them all other relief in law and in equity to which they may be entitled.

Respectfully submitted,

GREGOR | WYNNE | ARNEY, PLLC

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

Texas State Bar No. 00785289
SDTX No. 0018569
909 Fannin Street, Suite 3800
Houston, TX 77010
Telephone: (281) 450-7403
mwynne@gwafirm.com

Cameron Powell, Esq.*
DC Bar No. 00459020
Telephone: (503) 502-5030
cpowell@gwafirm.com

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

COUNSEL FOR DEFENDANTS

* Pro Hac Vice Pending

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing was served by CM/ECF e-service on December 27, 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 PLAINTIFF

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