UNITED STATES DISTRICT FOR THE
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

JOHN STUART,

Defendant.

21-CR-07-LJV-JJM

REPLY MEMORANDUM

INTRODUCTION

This reply memorandum is submitted in further support of John Stuart's Motion to Compel. Initially, this Court should reject the government's contention that the motion is untimely. First, the defense requested, and Judge Lawrence Vilardo granted, permission to file further motions. (Docket No. 49). The government took no position on that motion. (*Id.*) Second, the motions are only necessary because of the government's failure to provide adequate discovery in the first instance. Indeed, as a result of the motion to compel and any further discovery ordered by this Court, the defense anticipates filing further motions.

As for the substance of the response, the government suggests that much of the defendant's discovery requests rely on "pure speculation." Yet the documents provided to the defense[1] confirm the assertions that the defense has been making since it learned through its own independent investigation that the search warrant affidavit presented to the issuing-search-warrant Magistrate Judge in this case were nearly identical to dozens and dozens of warrant

[1] These documents are subject to a protective order, but will be provided to the Court under separate cover. Any reference to information from the protected will be redacted in the public filing.

applications throughout the country. Indeed, the documents provided by the government as a result of the motion to compel confirm:

- The warrant presented to Judge Roemer was a batch warrant, drafted almost entirely by an FBI agent other than Agent Hockwater, who signed it.
- Nearly identical affidavits were submitted throughout the country.
- Mr. Stuart's case arose out of a broad, international cooperative investigation into a server hosting several child-pornography websites.
- The website at issue in this case is called [redacted]. This is significant because [redacted] is one of the websites hosted by the server that the defense has been arguing was located in a country other than the [redacted].

Thus, far from "pure speculation," the defendant's assertions have been confirmed by the documents disclosed to date.

Yet, as explained below, the government's disclosures continue to fall short. At the time of the search warrant application the government had disclosed to the issuing judge (and subsequently to the defense) only the tip of the iceberg. These recent disclosures are measured and carefully crafted to reveal only a small fraction more of that iceberg. Indeed, the government continues to suggest that the U.S. was merely the idle beneficiary of a lucky tip. But the defense's investigation reveals it played a much larger role – one that was certainly not disclosed at the time of search warrant application and one which it continues to try to hide.

ARGUMENT

There was a collaborative effort involving the United States well before the tip arrived from the [redacted], and information related to that investigation should have been disclosed earlier. It must be disclosed now.

The government's main contention in refusing to provide further discovery is twofold: First, that further discovery is unwarranted because the defense's claim that the FBI and other countries were working together is "unsupported," based entirely on an "inartful" choice of

words in a different case, and is "pure speculation." Second, that Agent Hockwater's assertion that the [redacted] did not "access, search, or seize any data from any computer in the United States" "belies" any suggestion that there can be any Fourth Amendment concern with the manner in which IP addresses were deanonymized.

The government continues to be less than forthcoming regarding the provenance of the tip. Although the tip itself may have come from the [redacted], a different country or countries were involved in seizing the server that hosted the [redacted] website (which the recently-provided documents confirm was the site allegedly visited by the IP address associated with Mr. Stuart). Further, the server itself was not located in the [redacted]. Although the government attempts to sidestep this important fact, it cannot deny it.

Thus, asserting that the [redacted] did not "access, search, or seize any data from any computer in the United States" is meaningless. The government has made no assurances regarding the search, seizure, and data collection by the unidentified country where the server was actually hosted. The government has not yet identified what role the [redacted] had in acquiring the information that led to the tip. And it has not even acknowledged the existence of vast years-long collaborative investigation, which included the United States, that preceded and ultimately led to the information found in the tip.

The defense's independent investigation and government press releases about the identification and eventual seizure of that server reveal two key pieces of information: (1) years before receiving any "tip" regarding IP addresses from the [redacted] in this case, the FBI was significantly involved in the international investigation that led to both the identification and seizure of the server; and (2) finding the server, shutting it down, and de-anonymizing the IP address that had visited the website was clearly a joint venture and operation between the U.S.

and other countries' law enforcement agencies.

Indeed, the ultimate unearthing of the IP address in this case was the result of an international collaboration beginning sometime in 2017 between INTERPOL, Europol, and law enforcement agencies in the U.S., Austria, France, Italy, the United Kingdom, Australia, Canada, and Brazil.[2] The investigation eventually led to the arrest of a man known by his online moniker "Twinkle" in Portugal. [3] "Twinkle" was an administrator on a child sexual abuse hidden services site called [redacted]," one of five sites operated on the server.[4] In a press release, INTERPOL called the arrest "a textbook example of how international collaboration can put harmful individuals behind bars."[5]After his arrest, law enforcement was then able to track down another administrator of that site, who lived in Brazil.[6] In 2019 Brazilian authorities found a server that hosted five hidden-services websites focused on the sharing of child sexual abuse materials, including [redacted].[7]

The FBI and other U.S. law enforcement agencies were instrumental in the investigation. The FBI, for instance, helped Brazilian law enforcement locate the IP address of the individual hosting the server.[8] The FBI then used a deanonymization technique to

[2] "International collaboration leads to arrest of child sexual abuser in Portugal," INTERPOL (Jan. 23, 2020), https://www.interpol.int/News-and-Events/News/2020/International-collaboration-leads-to-arrest-of-child-sexual-abuser-in-Portugal; Mark Saunokonoko (Attached as Ex. A); "Elite Aussie unit helps catch elusive paedophile 'Twinkle' who ran darknet child abuse website [redacted]'" 9NEWS (Feb. 18, 2020), https://www.9news.com.au/national/queensland-police-taskforce-argos-helps-catch-twinkle-and-[redacted]-darknet-site/b5fa55c0-114f-4d66-a66c-045af0bee903. (The Australian Federal Police told *nine.com.au* it helped facilitate the global investigation, which included US, UK, French, Italian, Canadian, Brazilian and Portuguese law enforcement.").

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] "Operação Lobos," ANPR (Associação Nacional dos Procuradores de Republica (National Association of Public Prosecutors)) (Apr. 18, 2022), available at https://www.anpr.org.br/premiorepublica/votacao-sociedade/conheca-os-finalistas/26336-caso-volkswagen-contribuicao-com-os-orgaos-da-repressao-politica?tmpl=component&print=1. Attached as Exhibit B.

[7] *Id.*

[8] *Id.*

corroborate the identification of the server on the Tor network.[9]

Aided by the U.S.'s investigative techniques, Brazilian authorities were able to determine that the server was run by Lucas Batista dos Santos, known as "Lubasa."[10] Brazilian law enforcement arrested Lubasa and seized the server in June 2019.[11]

The [redacted] itself has said that [redacted] – the name that the [redacted] assigned the investigation – was a collaborative effort: "*Working with partners*, the [redacted] has identified a significant number of unique global internet protocol (IP) addresses on dark web sites; at least 5 percent of these IP addresses are believed to be in the [redacted]." (emphasis added).[12]

The government has never disclosed any information related to that search and seizure of the server – it refuses to even acknowledge its existence. Rather, this information was gleaned only through the defense's independent investigation.

This and further information is plainly discoverable under *Brady*, which renders discoverable any material that is favorable to the defendant. As relevant here, the government has never made any assurances whatsoever that the Brazilian investigation, search or seizure of the server complied with U.S. Constitutional standards. This information is also discoverable under Rule 16 because it goes to the heart of the investigation that led to the arrest of Mr. Stuart and a motion under *Franks v. Delaware* that the government misled the magistrate by omitting this deeply pertinent information. *See United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012); *see also United States v. Mitrovich*, 458 F. Supp. 3d 961 (N.D. Ill. 2020) (finding that the defendant had made a primafacie showing, for purposes of motion to

[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/an-inspection-of-the-national-crime-agency-criminal-intelligence-function.pdf.

compel discovery, that the joint venture doctrine applied and that malware had been used to obtain the defendant's IP address where U.S. law enforcement worked with Australian and New Zealand authorities to uncover IP addresses in the United States).

Accordingly, the government should be ordered to disclose to, or identify for, the defendant:

- All the foreign law enforcement agencies (FLA) and countries involved in all aspects of the investigation.
- What role each FLA had.
- U.S. law enforcement's full role, including what techniques were utilized and when they were utilized.
- Which U.S. agencies were involved and how.
- All information and documentation related to [redacted] in the possession of the prosecution team, as that term is defined by caselaw.
- What technique was used to locate, take down and seize the server.
- What technique was used to de-anonymize the website's IP address.
- Whether Mr. Stuart had account on the website in question.

Indeed, the government appears to have more information than it is sharing with the defense or the Court. In a case stemming from the same investigation, the government filed a complaint on the public docket that "outlined the law enforcement methodology used to unearth defendant's criminal conduct." *See* Government's Motion to Seal the Complaint, *United States v. Kidder*, No. 1:21-cr-00118-LN (W.D.N.Y. March 16, 2020), ECF No. 7 (attached as Exhibit C). Realizing the complaint contained "information that could reveal highly-sensitive law enforcement methods," the government then moved to seal the complaint. *See* Redacted Complaint, *United States v. Kidder*, No. 1:21-cr-00118-LN (W.D.N.Y. March

16, 2020), ECF No. 9.

The information contained in this complaint should also be disclosed.

Dated: Buffalo, New York
January 17, 2023

Respectfully submitted,

/s/ Jeffrey T. Bagley
Jeffrey T. Bagley
jeffrey_bagley@fd.org
Assistant Federal Public Defenders
Federal Public Defender's Office
300 Pearl Street, Suite 200
Buffalo, New York 14202
(716) 551-3341