UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**CRIMINAL NO. 21-CR-30028-MGM**
BENJAMIN SHACAR,	)	
	)	
	)	
Defendant.	)	
	)	
	)	

DEFENDANT'S REDACTED REPLY TO GOVERNMENT'S RESPONSE TO MOTION TO COMPEL DISCOVERY

This reply memorandum is submitted in further support of Benjamin Shacar's Motion to Compel.

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 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 was nearly identical to dozens of warrant 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 Robertson was a batch warrant, drafted almost entirely by an HSI agent other than Agent Yon, who signed it.
- Nearly identical affidavits were submitted throughout the country.
- Mr. Shacar's case arose out of a broad, international cooperative investigation into servers hosting 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 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 United Kingdom, 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 threefold: First, that the Defendant has failed to meet the burden of demonstrating the materiality of the items requested. Second, that the Defendant has not demonstrated that certain requested materials are in the custody or control of the government and that American agents participated in a foreign search, foreign officers acted as agents for their American counterparts, or that the conduct of foreign police shocks the judicial conscience. And third, the disclosure of certain material would imperil on-going investigations.

With respect to the first contention, the government claims that the Defendant has offered nothing more than speculation and "speculative theories" to support his demand for further discovery. The government complains that the Defendant has failed to authenticate certain exhibits filed in support of the motion to compel. The Defendant responds as follows:

Basis of Exhibits Filed in Support of Motion to Compel

Exhibit J – Comparison of Tip and Probable Cause Language.

Exhibit J to the Defendant's Motion to Compel provides a listing of cases throughout the country which used similar language in the warrant application affidavits used by law enforcement agencies. The cases in the exhibit specifically refer to the court and accompanying docket number, the defendant and/or address involved in the investigation, the tip language and probable cause language and the source of that language. There are 13 matters referenced in the listing. The government complains that the Defendant failed to authenticate this exhibit. In response, the Defendant has attached the documents referenced in Exhibit J with the exception of the search warrant application and affidavit related to 7850 Westmont Lane, McLean, Virginia. That matter is related to the case of *United States v. Sauders,* Eastern District of Virginia, 1:20-

cr-00143-TSE, said document being ordered sealed. The documents related to the remainder of the listed matters are attached as the following exhibits to this reply:

- Exhibit 1 – Motion to Suppress Evidence in *United States v. Bateman,* District of Massachusetts, 20cr10012IT;[1]
- Exhibit 2 – Complaint in *United States v. Stauffer,* Southern District of Illinois, 20mj4005RJD;
- Exhibit 3 – Affidavit regarding search warrant application and affidavit for 4068 Fairbanks Drive, Chipley Florida;
- Exhibit 4 – Affidavit regarding search warrant application for 5855 Hunting Lodge Road, Pleasant Garden, North Carolina;
- Exhibit 5 – Affidavit regarding search warrant application for 291 Old Brunswick Road, Gardiner, Maine;
- Exhibit 6 – Objection to Discovery Order and Request for Review by District Judge in *United States v. Keijzo,* District of Massachusetts, 20-cr-40036-TSH;
- Exhibit 7 – Affidavit regarding search warrant application for 6603 Crimson Lane, Barnhart, Missouri;
- Exhibit 8 – Affidavit regarding search warrant application for 234 South Magnolia Terrace, Lansing, Michigan;
- Exhibit 9 – Affidavit regarding search warrant application for 54 Spruce Street, # 6, Burlington, Vermont;
- Exhibit 10 – Complaint in *United States v. Clark,* Western District of Washington, MJ21-147;
- Exhibit 11 – Complaint in *United States v. David Corwin,* Eastern District of New York, 21-MJ-357;
- Exhibit 12 – Affidavit regarding search warrant application for 31 Adams Avenue, Rochester, New Hampshire.

These documents demonstrate multiple cases from across the country that rely on seemingly identical August 2019 tips from an undisclosed FLA that an IP address was used to visit a Tor hidden services website sometime in April or May 2019. The number of similar cases using similar, if not

[1] As the exhibits to the motion to compel were categorized alphabetically, the Defendant has categorized the exhibits numerically to this reply.

identical, language to the search warrant affidavit in Mr. Shacar's case indicates a large-scale, coordinated investigation into websites hosted on the Tor network akin to the Playpen investigation[2]

Exhibit K – FBI Documents

This case opening report FBI report dated January 13, 2017, was obtained through a FOIA request and filings in cases with search warrant application affidavits similar to the one in Mr. Shacar's case. See *Commonwealth v. Vincent Kiejo,* No. 20-cr-40036-TSH (District of Massachusetts, ECF # 172-10) This report documents a "preliminary investigation" into a Tor hidden service site with language identical to that found in the Yon affidavit. The report indicates that U.S. law enforcement opened an investigation into the service more than two years before the FLA relayed its "tip" that the suspect IP address had purportedly visited the target website.

Exhibit M – Interpol Press Release

This press release from Interpol can be found at the following website https://www.interpol.int/News-and-Events/News/2020/International-collaboration-leads-to-arrest-of-child-sexualabuser-in-Portugal. 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 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. 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. 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]

---

[2] *See* "The Playpen Cases: Mass Hacking by U.S. Law Enforcement," Electronic Frontier Foundation, available at https://www.eff.org/cases/playpen-cases-mass-hacking-us-law-enforcement.
[3] https://www.9news.com.au/national/queensland-police-taskforce-argos-helps-catch-twinkle-and-babyheart-darknet-site/b5fa55c0-114f-4d66-a66c-045af0bee903
[4] *Id.*
[5] *Id.*

Exhibit N – Brazilian Translation

This document is a translation of a Brazilian government press release related to the investigation, conducted by the Brazilian Federal Public Prosecutor's Office. The press release (in Portuguese) is attached as Exhibit 13 to this memorandum. After the arrest of Twinkle in Portugal, law enforcement was then able to track down another administrator of that site, who lived in Brazil. In 2019 Brazilian authorities found a server that hosted five hidden-services websites focused on the sharing of child sexual abuse materials.

Exhibit P – Stephen Murdoch Affidavit

Dr. Stephen Murdoch is a professor of Security Engineering at University College London whose research is focused on information security, particularly Internet privacy and payment systems security. He worked with the developers of Tor since 2004 and created the first version of the Tor Browser software in 2008. He continues to work with the Tor Project, the 501(c)(3) non-profit organization responsible for the development of the Tor network and associated software. He helped the Tor Project assess and improve the security and usability of Tor. Professor submitted an affidavit in the case of *United States v. Sanders*, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2.

In his affidavit, Agent Yon stated that the FLA [United Kingdom] assured U.S. law enforcement that that FLA had not "interfered with, accessed, searched, or seized any data from any computer in the United States.". This assurance, combined with the omitted fact that there was more than one FLA involved in the investigation, created the impression that no law enforcement agency, anywhere, had "interfered with, accessed, searched, or seized" data from a computer in the United States.

Professor Murdoch suggests that the specific IP address could not have been identified without running a Network Investigative Technique (NIT) or, in the alternative, an error-prone and unreliable traffic analysis technique. See Dr. Murdoch's declaration at ¶ 22-32, *United States v. Sanders*, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2 (Exhibit P to Motion to Compel) Professor Murdoch explains that "there are only two techniques for identifying the IP address of a user using Tor Browser properly: traffic-analysis (which can generate errors) or a NIT (which interferes with a user computer)." ¶ 23. A NIT works "by forcing the user's computer to disclose its IP address by connecting directly to a law-

enforcement server without using the Tor network." Id. at ¶ 27. A NIT "necessarily interferes with a user's computer wherever it is located." Id. at ¶ 32.

Traffic analysis, on the other hand, is a technique that attempts to "identify which user is communicating with which Onion Service by comparing patterns of when and how much data is sent (as opposed to looking at the content of the data, which is not visible to observers)." Id. at ¶ 17. Professor Murdoch states that before 2016, "traffic analysis on Tor was unreliable, but there were concerns that it might be possible in some cases." However, in 2016, Tor addressed this issue and introduced a new extension to its software that caused traffic analysis to "introduce more errors, both false positives (where a user is incorrectly identified as having visited the Onion Service) and false-negatives (where a user is incorrectly identified as not having visited the Onion Service)." Id. at ¶ 19. This measure, and others, have made it "even more difficult to use traffic analysis to de-anonymize Tor users." Id. at ¶ 21.

The use of either technique by the FLA which seized the server of the [Girland] website would significantly undermine the veracity of the affidavit and its probable cause showing. If traffic analysis was used to uncover the IP address, the undisclosed fact that the technique is inherently error-prone would significantly undermine the strength and reliability of the tip from . See id. at ¶ 22-32. In the case of *United States v. Raymond Dugan*, No. 21-cr-00127 (S.D. W.Va.), the government's forensic expert was unable to explain why Dugan's computer log supposedly showed the last 25 times TOR was either installed or used and showed use before and after the tip date of May 25, 2019, but did not show it was used on the actual date described in the tip. See Exhibit 14, pp. 10-13. No magistrate, had he or she been aware that this fundamentally unreliable technique was used to obtain the IP address, would find there was probable cause, especially where the tip about the IP address was not corroborated by any other facts.

Alternatively, the use of a NIT would reveal a substantial misrepresentation in the affidavit, which relies on Agent Yon's assurance that no computer in the United States had been searched. The deployment of a NIT is an unlawful warrantless search. See *United States v. Tagg*, 886 F.3d 579, 584 (6th Cir. 2018); *United States v. Anzalone*, 208 F. Supp. 3d 358, 366 (D. Mass. 2016), aff'd, 923 F.3d 1 (1st Cir. 2019). Had any law enforcement agency deployed a NIT to obtain the IP address without a warrant, the Magistrate could not have considered the results of that search in the probable cause analysis. See United States v. *Dessesaure*, 429 F.3d 359, 367

(1st Cir. 2005) ("[W]hen faced with a warrant containing information obtained pursuant to an illegal search, a reviewing court must excise the offending information and evaluate whether what remains is sufficient to establish probable cause.").

Agent Yon's omissions regarding the method used to obtain the IP address were material because if the omitted information – either that a NIT or an error-prone traffic analysis was used – was included in his affidavit, it would be "sufficient to vitiate probable cause." *United States v.Tanguay*, 787 F.3d 44, 49 (1st Cir. 2015). This Court may infer that the information was omitted recklessly because the omitted information was "critical to the probable cause determination." *United States v. Gifford*, 727 F.3d 92, 99-100 (1st Cir. 2013). Mr. Shacar is therefore entitled to a Franks hearing on this issue.

Exhibit Q – Email Correspondence between AUSA's

These materials were obtained via a Freedom of Information request in a related case – *United States v. Sanders*, 20-CR-143 (E.D. Va)[6] – reveal the United States was sharing information with law enforcement partners in Germany relative to its investigation into this server even before the U.S. claims to have received the "tip" in August of 2019. Since the filing of his motion to compel, the Defendant has obtained the entire contents of the government's response to the FOIA request and has attached it to this memo as Exhibit 15. Agents in the United States are discussing their operation with Germany in email exchanges dated June 13, June 14, June 20, June 21, and June 24 of 2019. (FOIA Response Ex. 15, pp. 3 11.). On June 24, 2019, for instance the Chief of the Federal Criminal Police in Germany emailed a redacted HSI agent, saying "good job! The report will be useful for us." (Id.) This is not a one way street.

Other emails released in this batch demonstrate that at least as early as 2018, HSI and the FBI were working together on projects they called "good listener" and were emailing documents about "guard research." (Id., at p. 24) In the world of Tor, the entry node is often called the guard node; it is the first node to which the Tor client connects. One email purports to show how "good listener" actually works, with sections on "Background" and "Methodology." This document is dated September 2018, well before the United States claims to have gotten a lucky "tip."

[6] Zackary Sanders was accused of accessing a server containing child exploitation materials – and was allegedly located as a result of the same "tip" from the [redacted] – as Benjamin Shacar.

It must also be noted that in the FOIA response cover sheet, HSI indicates that it was providing only 71 (heavily redacted) pages. Another "935 pages have been temporarily set aside as a potential future supplemental production, pending confirmation of the existence of a court seal on those documents." (Id.)

Among the 71 redacted documents that were provided (only 7% of the total production that HSI itself deemed relevant), is an email chain dating back to July 1 of 2019 where FBI and HSI agents are discussing a draft search warrant affidavit "that has not been signed off on yet." (Id., pp. 70-71.) This draft affidavit, it appears, eventually becomes the boilerplate affidavit ("Tor Op Go By," in their verbiage) that has been used in search warrant applications like the one for Mr. Shacar across the county. This is critical because the affidavit was being drafted before the U.S. received the "tip" in August of 2019. Although seemingly all names have been redacted, Agent Squire, who received the award from the [redacted] for his contribution to [redacted] received an email about the affidavit. (Id., p. 23).

Evidence of U.S. Participation in the Search

The government still wants the defense and this Court to believe this tip was a "one way street." It was nothing of the sort. A United States law enforcement officer has received an award for work done on the very operation in the where the deanonymization is alleged to have occurred. The United States admits that it played a critical role in uncovering the server that hosted the website. The U.S. is working on projects to uncover Tor users – and even drafting search warrant affidavits – well before the "tip" was received. All along, the U.S. was actively providing information to other countries. Despite all this, the government continues to assert that it did nothing more than receive a "tip," and that notions of agency or joint venture are mere "speculation." These government assertions can no longer be countenanced. Rather, it is becoming increasingly clear that the warrant application was intentionally drafted in a manner to conceal the United States' highly active role in this operation – likely in an effort to avoid having to disclose the constitutional concerns that a hearing would reveal.

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 was involved in seizing the server that hosted the. 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 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 that years before receiving any "tip" regarding IP addresses from the in this case, the FBI was significantly involved in the international investigation of Tor websites that led to both the identification and seizures of servers.

The [redacted] itself has said that [redacted] – the name assigned the investigation – was a collaborative effort. (Exhibit 16)

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 investigation, search or seizure of the server conducted by the second FLA 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. Shacar 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 prima facie showing, for purposes of motion to 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

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 17). 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.

This Court must hold a hearing to determine whether the search shocks the conscience, as well as to determine the amount of U.S. involvement and cooperation in the unconstitutional search.

The government contends that Mr. Shacar has not shown that the collection of requested documents shocks judicial conscience. Although the Fourth Amendment and its exclusionary rule generally do not apply to the law enforcement activities of foreign authorities acting in their own country, the concepts do apply where (1) the conduct of foreign officials in acquiring the evidence is so extreme that it shocks the judicial conscience, and second, (2) where U.S. cooperation with foreign law enforcement officials may implicate constitutional restrictions. *United States v. Valdivia,* 680 F. 3d 33, 51 (1st Cir. 2012); *United States v. Getto*, 729 F.3d 221, 228 (2d Cir. 2013).

This Court cannot answer these questions without a hearing. As an initial matter, the prosecution in this case has claimed that the information leading to the search warrant application came from a FLA which did not seize the server hosting the target website and thus simply relied upon the tip alone. As a result, the government does not know how the hidden IP address was recovered. If that is the case, the government cannot, therefore, assure this Court that the manner in which it was uncovered would not shock the conscience. It is still unknown how the IP addresses were deanonymized – an ability that only nation states appear to have. To this point, the prosecution is only saying that the [redacted] provided a "tip" to the United States that certain IP addresses accessed certain Tor websites.

Second, we now know that the United States government was more than a passive recipient of a generous tip, despite the misleading nature of the search warrant application meant to leave this impression. As noted in previous briefing, there was long-standing collaboration between at least, the [redacted], [redacted] and the United States and possibly other FLA's. New facts demonstrating this collaboration continue to be unearthed. The [redacted], the law-enforcement aim of the [redacted] government tasked with investigating online crimes, code-named their investigation in this matter Operation or Project [redacted]. According to the [redacted], [redacted] is the [redacted]'s project tackling child sexual exploitation offending on the dark web ... 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]" [redacted], An inspection of the [redacted]'s criminal intelligence function, p. 11 (July 2020) (attached as Ex. 16).

At least one Homeland Security Agent, Gregory Squire, was deeply involved in that operation. Indeed, Agent Squire drafted one of the first - if not the first - affidavits in support of a criminal complaint charging an American with crimes associated with this operation. See United States v. Bateman, 20-CR-10012 (D. Mass.) (affidavit attached as Ex. 18). Agent Squire has a LinkedIn account in which he highlights an award bestowed on him by Director General Graeme Bigger[7] of the [redacted] for his contributions to [redacted]. (See Exhibit 18) As

[7] https://www.nationalcrimeagency.gov.uk/news/director-general-graeme-biggar-launches-national-strategic-assessment

described above with respect to the government's response to a FOIA request, FBI and HSI agents are discussing a draft search warrant affidavit that appears, to become the boilerplate affidavit ("Tor Op Go By," in their verbiage) that has been used in search warrant applications like the one for Mr. Shacar across the county. In the document production related this communication where seemingly all names have been redacted, Agent Squire, who received the award from the [redacted] for his contribution to [redacted] received an email about the affidavit. (Ex. 15, p. 23).

It bears repeating that the warrant application leading to the search of Mr. Shacar's home is drafted to leave the impression that the U.S. was not involved at all; that they were the passive receipt of a lucky tip from a "foreign law enforcement agency." The government continues to assert that this was a case of "one-way information sharing" where the U.S. simply received information from the [redacted] The defense's investigation reveals that to be false. Agent Squire was so intimately involved in the operation that the leader of this "foreign law enforcement agency" awarded him a commendation. Homeland Security (HSI) agents do not get commendations for passively receiving information; they get commendations for having a pivotal role in acquiring it. This fact alone establishes at least enough to warrant a hearing on the extent of the cooperation, the degree to which the was an agent of the United States, and the nature of the investigation that led to the deanonymizing of Mr. Shacar's and thousands of others' IP addresses.

If more were needed, the United States Department of Justice itself touts among its "accomplishments" that it continues to "lead and coordinate strategic enforcement operations and/or prosecutions including those involving Arlan Harrell, John Brinson, Moises Martinez, and Keith Lawniczak who were active members of several Tor-network-based child exploitation websites. See DOJ Performance Budget FY 2024 Congressional Submission, p. 29 (attached as Ex. 19)

The government has not shown that disclosure of the requested materials will imperil ongoing investigations

The government makes a general claim that disclosure of some of the requested information would imperil ongoing investigations. The government cites to *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987) in support of its claim that the information is privileged. As described in Agent Yon's affidavit in support of application for search warrant,

the target website went offline in March 2020, over four years ago. Based upon that representation, it appears that the information requested does not relate to further investigations of the target website as it is no longer operative.

The authority to withhold information about sensitive investigative techniques is a qualified privilege. As the court in Cintolo stressed, the privilege can be overcome by a sufficient showing of "need" and the "necessity determination" requires a case by case balancing process controlled by 'the fundamental requirements of fairness. Accordingly, "a defendant seeking to such information should ordinarily show that he needs the evidence to conduct his defense and that there are no adequate alternative means of getting at the same point" Id. In this case, Mr. Shacar, despite his own investigative attempts, has no other way of obtaining this information. In terms of need, Mr. Shacar has set forth the reasons for this request in terms of challenging the legitimacy of the search in light of the omissions from the search warrant application and his need to know the process by which the FLA which seized the server obtained the information which led to the tip from the [redacted]. Mr. Shacar contends that his need to obtain the requested information outweighs the government's claimed privilege.

CONCLUSION

For the reasons described above as well as for the reasons stated in his Motion to Compel Discovery, the Defendant respectfully requests that this Honorable Court allow said motion.

Respectfully submitted,

BENJAMIN SHACAR

/s/ William J. O'Neil

WILLIAM J. O'NEIL
Attorney for the Defendant
280 N. Main St., Ste. 6
East Longmeadow, MA 01028
(413) 224-2694
BBO#:548445

CERTIFICATE OF SERVICE

I hereby certify that true copies of this document will be served on the registered parties through the ECF system on this date March 29, 2024.

/s/ William J. O'Neil
William J. O'Neil
280 N. Main Street, Ste. 6
E. Longmeadow, MA 01028
(413) 224-2694
BBO#: 548445