IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,

v.

MICHAEL A. SUSSMANN,

Defendant.

Case No. 1:21-cr-00582

DEFENDANT'S MOTION TO PRECLUDE EXPERT TESTIMONY SET FORTH IN THE SPECIAL COUNSEL'S SUPPLEMENTAL EXPERT DISCLOSURE

Defendant Michael A. Sussmann, by and through his counsel, hereby moves to exclude certain testimony set forth in the Special Counsel's Supplemental Expert Disclosure.

The Court has previously ruled that FBI Special Agent David Martin should be permitted to testify about certain background topics, namely, information "necessary to understand the relevant data"; the "type of conclusions that can be drawn from analyzing the kind of data Mr. Sussmann shared with the FBI"; and "the methods investigators would use to validate or further examine such data." Order at 5, ECF No. 95 (hereinafter, "Order"). The Court further stated that the six topics identified in the Special Counsel's opposition to Mr. Sussmann's motion to exclude (hereinafter, "Opposition") "appear to fall within those parameters." *Id.*; *see also* Opp. at 3-4, ECF No. 69. But the Special Counsel is construing the Court's order in a way that goes beyond the permitted parameters.

Following entry of the Court's Order, the defense requested that the Special Counsel provide additional detail regarding the six topics about which he intends to offer expert testimony. The Special Counsel responded with nine categories of opinion testimony that he intends to elicit from Special Agent Martin regarding the fifth topic (*i.e.*, "the types of conclusions that can be drawn about (i) online activities based on a review of DNS data, and (ii) the origins and sources of DNS data"). Three of those nine categories appear to fall within the ambit of the Court's ruling. But six of those categories go well beyond permissible testimony regarding the "the type of conclusions that can be drawn from analyzing the kind of data Sussmann shared with the FBI." Instead, they appear designed to elicit testimony from Special Agent Martin that will cast doubt on the accuracy of the data Mr. Sussmann presented to the FBI, the conclusions Mr. Sussmann presented to the FBI, and the materiality of the alleged false statement. Mr. Sussmann respectfully contends that these six categories go beyond what is proper background and accordingly moves to preclude such testimony.

BACKGROUND

In the Special Counsel's initial expert disclosure dated March 30, 2022, he stated that Special Agent Martin intended to testify regarding: "the basic mechanics, architecture, and terminology of the DNS system and DNS data;" how private companies and entities maintain DNS "resolvers;" specific examples of DNS data in order to describe the meaning of such data; the nature and types of conclusions that can and cannot be drawn about persons' or entities' online activities based on a review of DNS data; and "the analytic significance and conclusions that can be drawn based on the provenance and origins . . . of DNS data." *See* Letter from J. Durham to S. Berkowitz and M. Bosworth at 1-2 (Mar. 30, 2022), ECF No. 66-1. In addition, the Special Counsel suggested that Special Agent Martin would potentially testify regarding the authenticity of the data provided to the FBI and "the possibility that such purported data was fabricated, altered, manipulated, spoofed, or intentionally generated for the purpose of creating the false appearance of communications." *Id.* at 2.

On April 8, 2022, the defense filed a motion to exclude proposed expert testimony—objecting specifically to testimony regarding the accuracy of the data and conclusions provided to the FBI—and requesting additional information regarding the proposed testimony regarding DNS data. *See* Def.'s Mot. to Exclude Gov't's Proposed Expert Witness Test. at 2, 3 n.3, ECF No. 66. In response, the Special Counsel described the testimony Special Agent Martin intends to offer regarding DNS data and TOR as falling into the following six categories:

- A description to the jury about the basic mechanics, architecture, and terminology of the DNS system and DNS data so that the jury can understand the various technical terms and concepts which appear in documents and other evidence that the Government intends to offer;
- An explanation to the jury regarding how certain private companies and entities maintain DNS "resolvers" and provide services involving DNS data, which includes processing and storing DNS data;
- A description of how private companies and entities gain access to DNS data and how they collect and commercialize that data;
- An explanation of certain examples of DNS data to assist the jury in understanding particular fields that appear within the data;
- A description to the jury concerning the types of conclusions that can be drawn about (i) online activities based on a review of DNS data, and (ii) the origins and sources of DNS data; and
- An explanation to the jury regarding the Onion Router ("TOR") and common terms used in connection with TOR, including the concept of a "TOR exit node" and the types of investigative steps and methods used for analyzing online activities involving TOR.

Opp. at 3-4.

On April 25, 2022, the Court ruled on Mr. Sussmann's motion, providing that it would allow expert testimony regarding (1) "background information necessary to understand the relevant data, including the 'basic mechanics, architecture, and terminology' of the kind of computer systems at issue"; (2) "the type of conclusions that can be drawn from analyzing the kind of data Sussmann shared with the FBI"; and (3) "the methods investigators would use to validate or further examine that data." Order at 5. The Court suggested that the six topics listed in the Special Counsel's Opposition "appear to fall within those parameters," but reserved ruling on objections to specific testimony. *Id.*

Following the Court's ruling, the defense requested that the Special Counsel provide additional detail about the testimony described in his Opposition. On May 6, 2022, the Special Counsel provided the defense with a supplemental disclosure identifying nine *new* topics, apparently under the umbrella of the previously described "description to the jury concerning the types of conclusions that can be drawn about (i) online activities based on a review of DNS data, and (ii) the origins and sources of DNS data." Opp. at 4; *see* **Ex. A**, Letter from J. Durham to S. Berkowitz and M. Bosworth (May 6, 2022) (hereinafter, "Supplemental Expert Disclosure").

The first four topics purportedly concern "the nature and types of conclusions that can – and cannot – be drawn about persons' or entities' online activities based on a review of DNS data." *Id.* at 1. Specifically, the Special Counsel apparently seeks to offer testimony from Special Agent Martin that:

1. The mere existence of a DNS lookup does not in and of itself reflect or prove the existence of actual communications between IP addresses (such as emails).
2. The mere existence of a DNS lookup also does not in and of itself reflect or prove the existence of an actual connection or exchange of substantive information between computers (*e.g.*, web browsing or file transfers).
3. There are a number of other events and causes that can trigger or initiate DNS lookups, including security scanning by automated systems/software, spam filtering, and other Internet "noise."
4. DNS communications can be "spoofed" through a process whereby a DNS lookup is made to appear falsely to originate from a particular IP address. In such a scenario, the automated response from the receiving IP address is directed to the "spoofed" domain/IP address.

Id.

The last five topics purportedly concern "the analytic significance and conclusions that can be drawn based on the provenance and origins (*e.g.* collection source) of DNS data." As to this category, the Special Counsel apparently seeks to offer testimony from Special Agent Martin that:

> 5. The nature and strength of the conclusions that can be drawn from a given DNS dataset depend, in part, on the "visibility" of the collection source, namely, the percentage of all global DNS traffic that is available to the collection source.
>
> 6. The more expansive the "visibility" of a collection source (*i.e.*, the greater percentage of global DNS traffic that is available to the source), the more conclusions (and stronger conclusions) can be drawn about a particular DNS dataset.
>
> 7. For example, if a company collecting passive DNS data has access to 100% of the world's DNS traffic, then searches or queries across its data would permit the collector of the data to draw definitive conclusions about the number of DNS lookups between particular IP addresses/domains. If a company has access to 2% of the world's DNS traffic, then searches or queries across its data would permit the collector of the data to draw only limited conclusions.
>
> 8. It is impossible to know the precise percentage of worldwide DNS data that a particular collection source covers.
>
> 9. It nevertheless can be important for an analyst of DNS data to consider the collection source and the visibility of that source.

Id. at 1-2. But the opinions set forth in the above topics 4-9 are not about "the type of conclusions that can be drawn from analyzing the kind of data Sussmann shared with the FBI" as permitted by the Court. Order at 5.[1] Instead, the Special Counsel apparently intends to use expert testimony to cast doubt on the specific data and conclusions that Mr. Sussmann provided to the FBI and opine on the materiality of the alleged false statement in this case.

ARGUMENT

The Special Counsel's supplemental topics 4-9 fall outside the bounds of what the Court ruled it would allow and instead veer into impermissible testimony apparently intended to prove

[1] Mr. Sussmann does not object to the Special Counsel's supplemental topics 1-3.

the alleged inaccuracy of the data and conclusions presented to the FBI by Mr. Sussmann and that it would have been material for the FBI to know about the origins the DNS data Mr. Sussmann provided. Such testimony should be excluded.

First, the Special Counsel's supplemental topics 4-9 go beyond "the type of conclusions that can be drawn from analyzing the kind of data Sussmann shared with the FBI." Order at 5. Topic 4—that DNS communications can be "spoofed"—is an opinion about how DNS data can be fabricated, not an opinion about how DNS data can be interpreted in the first place. Topics 5 through 8—that the nature and strength of the conclusions that can be drawn from a given DNS dataset depend on the "visibility" of the collection source; that the more expansive the "visibility" of a collection source, the more conclusions can be drawn; and that it is impossible to know the precise percentage of worldwide DNS data that a particular collection source covers—are opinions about the strength of conclusions that can be drawn from DNS data, not opinions about the types of conclusions that generally can be drawn (e.g., whether one computer was looking up the IP address of another). And topic 9—that someone analyzing DNS data would want to know about the source and collection of the data—likewise does not concern the types of conclusions that can be drawn from DNS data, but rather concerns opinions about the importance of knowing about where the data came from. Such topics are outside the scope of what the Court has said it would allow and, more generally, will not "help the trier of fact to understand the evidence or to determine a fact in issue." Fed. R. Evid. 702(a).

Second, even if generally related to the "types of conclusions that can be drawn" from DNS data, topics 4 and 5-9 really appear designed to use expert testimony to cast doubt on the accuracy of the specific data and conclusions that Mr. Sussmann provided to the FBI, an area of testimony that the Court has explicitly prohibited. *See, e.g.*, Order at 6 ("The Court will not risk confusing the jury and wasting time on a largely irrelevant or tangential issue."); *see also* Mot. Hr'g Tr. at 4:22-25 (Apr. 20, 2022) (suggesting that expert testimony about the accuracy of the data would only be relevant to the extent there was "something about the data on its face" that made it so that there was "no way that Mr. Sussmann could have reasonably believed in its accuracy").

Indeed, the Special Counsel appears to be attempting to get in through expert opinion precisely the type of testimony the Court has precluded from fact witnesses. *See, e.g.*, Op. & Order at 5, ECF No. 121 (hereinafter, "Op. & Order") (prohibiting the Special Counsel from offering exhibits suggesting that the collection of data was objectionable). For example, testimony about the Special Counsel's fourth supplemental topic regarding "spoofing" would suggest to the jury that the specific data Mr. Sussmann provided to the FBI could have been spoofed, even though there is no evidence suggesting that Mr. Sussmann had any such knowledge. The Court has already ruled that emails about potential spoofing constitute the "kinds of technical issues and conclusions about the data" that are not relevant. *See* Op. & Order at 10. Expert testimony on this topic should be excluded for the same reason.

Additionally, the Special Counsel's supplemental topics 5-8, regarding the "visibility" of the collection source of a given DNS dataset, appear designed to suggest that the conclusions offered in the white papers Mr. Sussmann provided to the FBI in fact lacked adequate support. For example, testimony describing that "more" and "stronger" conclusions can be drawn about DNS datasets that have "more expansive visibility" would tend to suggest to the jury that the data Mr. Sussmann provided was "less" and "weaker" because it only came from a certain set of sources. Likewise, there is no need to offer testimony that "[i]f a company has access to 2% of the world's DNS traffic, then searches or queries across its data would permit the collector of the data to draw only limited conclusions" unless the point is to suggest that only limited conclusions could be drawn from the actual data provided by Mr. Sussmann in this case. This is not background information that would aid the jury but instead information that would cast doubt on the integrity and scope of the data and conclusions that Mr. Sussmann provided to the FBI. *See* Order at 5; Op. & Order at 10 (explaining that "information about the accuracy of the data will not be admissible unless Mr. Sussmann opens the door" and that "conclusions about the data are not relevant" absent evidence that Mr. Sussmann knew about them).

Third, the Special Counsel apparently intends to offer expert testimony about the materiality of the false statement alleged in this case. Indeed, the Special Counsel's supplemental topic 9 regarding the importance of considering the collection source of DNS data is plainly being offered to prove materiality. But the Special Counsel did not disclose this topic in either his initial expert disclosure or Opposition, and the Court's ruling did not permit such testimony. The Special Counsel should not now be allowed to offer an entirely new expert opinion under the guise of eliciting testimony regarding the types of conclusions that can be drawn from a review of DNS data.

CONCLUSION

In short, the majority of the Special Counsel's Supplemental Expert Disclosure boils down to opinion testimony that appears to go beyond what the Court has otherwise permitted. For the reasons described above, the Special Counsel should not be permitted to elicit such testimony.

Dated: May 11, 2022

Respectfully submitted,

/s/ Sean M. Berkowitz

Sean M. Berkowitz (*pro hac vice*)
LATHAM & WATKINS LLP
330 North Wabash Avenue
Suite 2800
Chicago, IL 60611
Tel: (312) 876-7700
Fax: (312) 993-9767
Email: sean.berkowitz@lw.com

Michael Bosworth (*pro hac vice*)
LATHAM & WATKINS LLP
1271 Avenue of the Americas
New York, NY 10020
Tel: (212) 906-1200
Fax: (212) 751-4864
Email: michael.bosworth@lw.com

Natalie Hardwick Rao (D.C. Bar # 1009542)
Catherine J. Yao (D.C. Bar # 1049138)
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
Tel: (202) 637-2200
Fax: (202) 637-2201
Email: natalie.rao@lw.com
Email: catherine.yao@lw.com