IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	)	No. 1:15-cv-00662-TSE

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANTS' MOTION TO COMPEL DISCOVERY

Dated: March 26, 2018

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTION
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
OLIVIA HUSSEY-SCOTT
Trial Attorneys

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Counsel for Defendants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

RULES

INTRODUCTION

Defendants National Security Agency ("NSA") *et al.* hereby move pursuant to Federal Rule of Civil Procedure 37(a)(1), and District of Maryland Local Rule 104, to compel Plaintiff Wikimedia Foundation ("Wikimedia") to respond to three discovery requests—two interrogatories and one document request. These requests seek basic information about the Wikimedia communications that Plaintiff contends have been intercepted, copied, and reviewed in the course of NSA "Upstream" surveillance. The Government and its outside expert in the field of Internet communications technology seek these facts to assist the Government's expert in assessing the validity of the claim at the heart of Plaintiff's standing argument—that due to technical rules governing how the Internet works, the NSA "must be" intercepting, copying, and reviewing at least some of Plaintiff's communications during the Upstream process. Without those facts the Court will lack significant details relevant to determining whether it has jurisdiction over Plaintiff's claims. For its part, Plaintiff has interposed no valid objections to the Government's discovery requests. The Court therefore should order Plaintiff to respond to these requests by June 1, 2018, or another reasonable date certain.

BACKGROUND

Plaintiff seeks to contest the legality of Upstream surveillance, under which the NSA targets certain non-U.S. persons reasonably believed to be located outside the United States in order to acquire foreign-intelligence information. The NSA targets these individuals by acquiring online communications as they transit the "backbone" of the U.S. telecommunications network. Upstream surveillance is conducted under authority of Section 702 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a, pursuant to targeting and minimization procedures that must be approved by the Foreign Intelligence Surveillance Court as consistent with statutory requirements and the Constitution. Plaintiff nevertheless maintains that Upstream

collection exceeds the Government's authority under Section 702, violates the Constitution, and should be permanently enjoined. The threshold jurisdictional question to be resolved is whether Plaintiff has Article III standing to assert these claims.

I. Plaintiff's Standing Allegations

Although the technical operational details of Upstream surveillance remain classified, Plaintiff alleges that it involves an initial stage at which the NSA, using surveillance devices connected to the Internet "backbone," intercepts and copies a substantial number of the international online communications (including Plaintiff's own) transiting the U.S. telecommunications network, and scans them in-transit to identify communications containing selectors associated with the NSA's surveillance targets. First Amended Complaint (ECF No. 70-1) ("Am. Compl.") ¶¶ 46, 47, 49, 50. Plaintiff alleges that targeted communications, once identified, are ingested into Government databases and retained for analysis and dissemination of any foreign-intelligence information they contain. *Id.* ¶ 49. Plaintiff maintains that the initial stage of Upstream surveillance invades its Constitutional rights, *id.* ¶ 103, regardless of whether they are among the communications ingested, retained, read, and/or disseminated by the NSA.

In support of the assertion that the NSA intercepts, copies, and scans at least some of its communications, Plaintiff alleges that it engages in more than a trillion online communications each year, in three categories: (i) communications with its "community members," who read and contribute to its websites, (ii) internal "log" communications, and (iii) communications by its staff. *Id.* ¶ 86. Plaintiff asserts that the "sheer volume" and global distribution of its communications, together with the assumption that the NSA "must be" copying and reviewing all text-based communications that travel across any point on the Internet backbone that it monitors (to "reliably obtain" all communications to, from, or about targeted selectors), make it "virtually certain" that the NSA intercepts at least some of these communications. *Id.* ¶¶ 57–65.

On appeal from this Court's judgment dismissing the First Amended Complaint for lack of standing, *see Wikimedia Found. v. NSA*, 143 F. Supp. 3d 344 (D. Md. 2015), the Fourth Circuit held that Wikimedia (in contrast to its former co-plaintiffs) plausibly alleged interception of at least some of its communications. *Wikimedia Found. v. NSA*, 857 F.3d. 193, 210–11 (4th Cir. 2017). The Court of Appeals based this conclusion on three "key" allegations that it held were entitled to a presumption of truth at the pleading stage: (1) that, given their great volume and worldwide distribution, Plaintiff's "communications almost certainly traverse every international [Internet] backbone link connecting the United States with the rest of the world"; (2) that, due to alleged "*technical rules of how the Internet works*," the NSA "must be copying and reviewing all the international text-based communications that travel across a given link" on which the NSA is conducting Upstream surveillance if it is to "reliably" conduct that surveillance; and (3) that the NSA is conducting surveillance on "at least one" Internet backbone link. *Id*. (emphasis added). The Court of Appeals held that these allegations, taken together, made it sufficiently plausible, at the pleading stage, that the NSA is intercepting, copying, and reviewing at least some of Wikimedia's online communications. *Id.* at 211.

II. "Technical Rules" Governing Transmission of Internet Communications

Thus, the threshold question of Plaintiff's standing turns in essential part on technical details of how Plaintiff's online communications transit the Internet. While the import of these technical details is properly a subject of elaboration by the parties' experts, those details provide context for the parties' discovery disputes. Of relevance here are (i) Internet communications "protocols," (ii) Internet Protocol ("IP") addresses, and (iii) encryption.

Generally speaking, to send a communication on the Internet, the transmitting device (*e.g.*, a personal computer, a cell phone, or the computer—a.k.a. "server"—on which a website is physically stored) first converts the communication into one or more "packets," relatively small

bundles of digital information. *See* Am. Compl. ¶ 42. Each packet contains a portion of the communication's contents, together with address and routing information used to direct the packet across the Internet to its destination. *See id*. ¶ 43. This address and routing information includes the packet's source and destination Internet Protocol (IP) addresses, which are numeric identifiers corresponding to particular computers, devices, or systems connected to the Internet. IP addresses may be analogized to the address and return address on an envelope sent through the mail, *see id*., or to telephone numbers identifying the source and destination of a call.

Once a communication has been converted into these constituent packets, the packets travel online through a series of "routers," electronic devices that direct traffic on the Internet. Routers use the destination IP address contained in each packet to direct the packets from one router to the next until they reach the computer (or other device) associated with the destination IP address. *See id.* ¶¶ 42–43. The destination device then reassembles the packets into the original communication. *See id.*

This process is made possible by the use of a number of different standardized Internet communications "protocols." In broad terms, protocols are simply agreed-upon sets of rules governing how Internet communications are to be structured—including what information is to be included in a packet and how it is organized. *See id.* ¶ 43. The use of standardized protocols ensures that computers receiving Internet packets can correctly interpret them and convert them back into the original communications. *See id.* Take, for example, the Hypertext Transfer Protocol ("HTTP"), historically the basic protocol used to transmit information contained on websites (such as Wikipedia). *See id.* To transmit a page from a website to an Internet user, the server hosting (containing) the website would break the webpage down into packets according to the rules of the HTTP protocol (and the protocols HTTP uses in turn, TCP and IP). When the destination computer received the packets, it would recognize them as HTTP data, and then

follow the rules of the HTTP protocol to convert them back into a webpage displayed on the user's device. *See id.*

Because the most efficient way of transmitting information across the Internet can depend on the type of information being transmitted, different protocols are generally used to transmit different types of information. *Id.* Different protocols are also typically assigned different "ports." Ports, like IP addresses, are numeric strings contained in the addressing information of each communications packet. While IP address are used to route a packet to a destination device, ports are used by the destination device to ensure that different kinds of communications, once received, are directed to the correct applications (programs) capable of interpreting and displaying them. *See id.* For example, HTTP packets historically have been assigned Port 80 by default, so that when a user requested a webpage, the constituent packets were directed to her web browser (such as Internet Explorer) rather than a program on her computer designed for reading e-mail (such as Microsoft Outlook).

Internet communications also now often rely on encryption, which means essentially the same thing in this context as in others: encoding parts of Internet packets (but not the address and routing information) through use of a cipher, with the intention of rendering them unreadable except by the destination computer. Thus, today, webpages—including those of Plaintiff, *id.* ¶¶ 88–91—often use the HTTPS protocol (for HTTP Secure), which combines HTTP with an encryption protocol to prevent webpage information from being read or changed in transit. Despite its relation to HTTP, the HTTPS protocol has been assigned a different port, Port 443.

III. The Government's Discovery Requests and Plaintiff's Responses

After the Fourth Circuit's ruling, the Court held a status conference on September 22, 2017, at which it concluded that discovery on remand should be limited initially to jurisdictional issues, followed by resolution of the jurisdictional question, before the case proceeded (if at all)

to litigation on the merits of Plaintiff's claims. Thereafter, the Court issued an Order, dated October 3, 2017 (ECF No. 117), granting the parties five months' time for jurisdictional discovery ending on March 17, 2018. The Court subsequently extended this discovery period to April 17, 2018. Mar. 15, 2018, Order (ECF No. 123).

The Government served interrogatories and document requests on Plaintiff on November 16, 2017, followed by additional interrogatories and document requests served on December 20, 2017. Plaintiff served its written objections and responses to the Government's requests on January 11 and 26, 2018, respectively, and produced responsive documents on February 12, February 16, March 6, and March 23, 2018. The Government served a single, final interrogatory on Plaintiff on March 16, 2018; on March 22, 2018, Plaintiff objected to this final interrogatory and indicated that, based on these objections, it would not provide a response.

In February and March 2018, the parties met and conferred extensively about the various ways in which the Government contends Plaintiff's discovery responses are deficient. Plaintiff has addressed some of these deficiencies, but others remain. Rather than moving to compel all responses to which the Government believes it is entitled, Defendants have elected to move only for a limited set of information about an issue fundamental to this case: basic technical facts about Plaintiff's communications that Defendants' outside expert in Internet communications technology has determined are pertinent to assessing Plaintiff's claim that, under the "technical rules" of the Internet, the NSA "must be" intercepting, copying, and reviewing at least some of its communications. *Wikimedia*, 857 F.3d at 210. In particular, the Government and its expert seek to know (i) the protocols used to transmit the categories of communications that Plaintiff contends are subjected to Upstream surveillance, (ii) Plaintiff's IP addresses to or from which these communications are sent, and (iii) whether and how these communications are encrypted.

The Government also seeks to address Plaintiff's claims regarding the volume and worldwide distribution of its communications—another mainstay of its standing argument. *See id*. For this purpose, the Government seeks, as to each of the three categories of Wikimedia communications that Plaintiff contends are subjected to Upstream surveillance, information about the volume of those communications and the countries to and from which they are sent.

To these ends, the Government seeks to compel responses to three related discovery requests, Office of the Director of National Intelligence ("ODNI") Interrogatory Nos. 14 and 19, and Department of Justice ("DOJ") Request for Production No. 1. Principal among these is ODNI Interrogatory No. 19, through which the Government, following extensive discussions between the parties intended to narrow their differences over discovery, sought to reduce to its essence the information it is seeking in a single, straightforward interrogatory, as follows:

> NSA Interrogatory No. 3 requests that Plaintiff identify each category of Wikimedia international, text-based, Internet communications that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance. For the period January 1, 2017, to the present, please describe the communications in each such category by stating:
>
> a. each communications protocol used to transmit Wikimedia communications in that category;
> b. the number, to the extent it is known or can be estimated, of Wikimedia communications in that category using each protocol;
> c. to the extent known, the countries to and from which Wikimedia communications in that category, using each protocol, are transmitted;
> d. whether and by what means communications in that category using each type of protocol are encrypted; and
> e. the Internet Protocol (IP) addresses or address blocks used by Wikimedia for purposes of transmitting or receiving communications in that category.
>
> If Plaintiff does not intend at summary judgment or trial to offer proof that communications in a given category that use a given protocol are intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, then it need not identify, quantify, or otherwise respond to this interrogatory concerning communications in that category using that protocol.

See Ex. 1, Pl.'s Resp. to ODNI Interrogatory No. 19, at 8.

Prior to serving ODNI Interrogatory No. 19, the Government served ODNI Interrogatory No. 14 on Plaintiff, which similarly asked Plaintiff to state, for each category of its communications that it maintains is subject to Upstream surveillance, "what portion (percentage) of that category of Wikimedia communications is encrypted, and in what manner . . . ." *See* Ex. 2, Pl.'s Resp. to ODNI's Second Set of Interrogatories, at 9. DOJ Request for Production No. 1 seeks documents sufficient to show this same information. *See* Ex. 3, Pl.'s Resp. to DOJ's First Set of Requests for Production, at 8.[1]

Plaintiff's primary objection to these requests is that they seek information irrelevant to jurisdiction, or more precisely that they seek "information that is not reasonably calculated to lead to the discovery of admissible evidence" and "information that exceeds the scope of jurisdictional discovery." Plaintiff also makes a host of boilerplate subsidiary objections: *e.g.*, that the requests are overly broad, unduly burdensome, not proportional, vague, and improperly duplicative. *See* Ex. 1, Pl.'s Resp. to ODNI Interrogatory No. 19, at 9; Ex. 2, Pl.'s Resp. to ODNI's Second Set of Interrogatories, at 9–10; Ex. 3, Pl.'s Resp. to DOJ's First Set of Requests for Production, at 8. The parties have met and conferred regarding these three discovery requests, and Plaintiff has indicated that it will not respond to these requests absent an order of the Court. Accordingly, the Government now moves to compel responses.

ARGUMENT

The Government's discovery requests at issue seek straightforward technical information about the basic nature of the communications that Plaintiff itself asserts, for purposes of attempting to establish its standing, are intercepted, copied, and reviewed in transit during the

[1] The Government also served an interrogatory, ODNI Interrogatory No. 15, seeking the IP addresses of the Wikimedia servers, located in the United States, to which its "log" communications are transmitted. Plaintiff responded with the IP address information requested, and ODNI Interrogatory No. 15 is not a subject of this motion.

course of NSA Upstream surveillance. For the reasons discussed below, the Government's outside expert has determined that this information is pertinent to assessing one of the three pillars on which the Fourth Circuit held that Plaintiff's claim of standing rests—that due to "technical rules" governing how communications are transmitted on the Internet, the NSA "must be" intercepting, copying, and reviewing at least some of its online communications. The Court should require, therefore, that it be produced.

I. Basic Technical Information about Plaintiff's Communications That the Government's Expert Has Determined Is Pertinent to Analysis of Plaintiff's Standing Argument Is Relevant to Whether the Court Has Jurisdiction Over Plaintiff's Claims.

Plaintiff primarily resists providing information regarding the protocols, IP addresses, and encryption of its communications by arguing that this information is irrelevant to the issues of jurisdiction upon which the Court has authorized discovery. "Discovery under the Federal Rules of Civil Procedure," however, "is broad in scope and freely permitted." *Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs., Inc.*, 334 F.3d 390, 402 (4th Cir. 2003) (citation omitted). The Federal Rules of Civil Procedure provide that a party

> may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.

Fed. R. Civ. P. 26(b)(1). For purposes of discovery, relevance is defined expansively:

> Normally, evidence is relevant if it has the tendency to make the existence of any fact consequential to the determination of the action more probable or less probable. In the context of discovery, however, courts construe relevancy more broadly. Relevant information encompasses "any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." *Indeed, for discovery purposes, the general subject matter of the litigation, rather than the pleadings or merits of the case, govern the scope of relevant information.*

Santos v. Crowell, 2016 WL 6068082, at *4 (D. Md. Oct. 17, 2016) (emphasis added) (citations omitted). Thus, "[a] request for discovery should be considered relevant if there is any possibility that the information sought may be relevant to the subject matter of the action." *Cappetta v. GC Servs. Ltd. P'ship*, 2008 WL 5377934, at *2 (E.D. Va. Dec. 24, 2008) (citation omitted); *see also Martin v. Bimbo Foods Bakeries Distribution, LLC*, 313 F.R.D. 1, 5 (E.D.N.C. 2016) ("[R]elevance has been broadly construed to encompass any possibility that the information sought may be relevant to the claim or defense of any party.") (citation omitted)).

When a party resists discovery on the ground that the requested discovery is irrelevant, "the burden is on the resisting party to establish the lack of relevance by demonstrating that the requested discovery (1) does not come within the broad scope of relevance as defined under Fed. R. Civ. P. 26(b)(1), or (2) is of such marginal relevance that the potential harm occasioned by discovery would outweigh the ordinary presumption of broad discovery." *Kantsevoy v. LumenR LLC*, 2017 WL 4516553, at *4 (D. Md. Oct. 6, 2017) (quoting *United Oil Co. v. Parts Assocs., Inc.*, 227 F.R.D. 404, 412 (D. Md. 2005)); *see also Desrosiers v. MAG Indus. Automation Sys., LLC*, 675 F. Supp. 2d 598, 601 (D. Md. 2009) ("The burden is on the party resisting discovery to explain specifically why its objections, including those based on irrelevance, are proper given the broad and liberal construction of federal discovery rules."); *Cappetta*, 2008 WL 5377934, at *2 ("The burden is on the party resisting production to show specifically how. . . each interrogatory is not relevant.") (citation omitted).

Plaintiff cannot discharge this burden because the categories of information the Government seeks—and that its expert says are pertinent to formulating his opinion—are relevant to show that Plaintiff cannot substantiate the second of the three allegations the Fourth Circuit identified as "key" to supporting its standing. Specifically, as noted earlier, the Court of Appeals concluded that Plaintiff had plausibly pled standing by alleging that the Government

had intercepted its communications because: (1) given their volume and worldwide distribution, Plaintiff's "communications almost certainly traverse every international [Internet] backbone link connecting the United States with the rest of the world"; (2) due to "technical rules of how the Internet works," the NSA "must be copying and reviewing all the international text-based communications that travel across a given link" on which the NSA is conducting Upstream surveillance if it is to "reliably" conduct that surveillance; and (3) the NSA is conducting surveillance on "at least one" Internet backbone link. *Wikimedia.*, 857 F.3d at 210–11.

Thus, if the NSA is not necessarily copying and reviewing all communications traveling across such a point, Plaintiff cannot prove its second "key" allegation, and Plaintiff's theory of standing collapses. Accordingly, any information that could serve to undermine this allegation necessarily has bearing on the Court's jurisdiction. Each piece of technical information about Plaintiff's communications that the Government is moving to compel—their transmission protocols, IP addresses, and whether and how they are encrypted—is relevant for this reason.

First, the protocols used to transmit particular types of Plaintiff's communications are relevant because certain protocols are associated with types of communications in which an entity conducting surveillance, for one reason or another, might have little interest. Electronic devices that might be used to conduct online surveillance can be configured (programmed) simply to ignore—which is to say, not to intercept, copy, or review— communications using those protocols. For example, as described above, the HTTPS protocol used by many websites, including Plaintiff's, is an encrypted protocol designed to render HTTPS communications unreadable except by a destination computer. An entity seeking to conduct surveillance on the Internet that lacks the ability to decipher encrypted HTTPS communications may well decide to program its surveillance equipment to disregard such communications altogether, rather than burden the finite processing capacity of its equipment with communications that it cannot read.

This can readily be accomplished because HTTPS communications, like communications using other protocols, are assigned a particular communications "port"—in the case of HTTPS, Port 443. Electronic devices that might be used for purposes of Internet surveillance are easily configured to "block," or ignore, communications assigned to designated ports. Thus, if the NSA lacked the ability to decipher HTTPS communications—and whether it does or not is a classified fact—then nothing in the "technical rules of how the Internet works," *Wikimedia*, 857 F.3d at 210, would prevent the configuration of devices used in connection with Upstream surveillance to exclude HTTPS communications from those that are intercepted, copied, and reviewed. (Of course, as noted above, the technical operational details of how Upstream surveillance is actually conducted remain classified.)

The IP addresses assigned to Wikimedia's communications are relevant for similar reasons. Organizations such as Plaintiff that operate popular websites or that otherwise have a fixed presence on the Internet are often assigned "static," meaning long-term, IP addresses. Electronic equipment that might be used to conduct online surveillance can be configured to ignore communications with particular source or destination IP addresses, meaning they could be operated so as to disregard communications to or from entities of low interest. Inversely, surveillance devices could be configured to intercept, copy, and review only those communications to or from IP addresses assigned to entities of high interest. Either way, if the NSA deemed communications to and from Wikimedia's websites to be of low foreign-intelligence value, then nothing in the technical rules of the Internet would prevent the configuration of equipment used in connection with Upstream surveillance to ignore all communications having source or destination IP addresses associated with Wikimedia.

Indeed, Plaintiff has already acknowledged that the NSA may not actually be copying and reviewing all Internet communications that pass through any point on the Internet as part of

Upstream surveillance. Rather, according to Plaintiff, the NSA may use certain technical criteria (criteria such as the technical information the Government is moving to compel) to entirely exclude from its Upstream surveillance process categories of Internet communications of little or no intelligence value:

> [L]arge swaths of internet traffic . . . are not amenable to the text-based searches conducted in the course of Upstream surveillance and are likely of no foreign-intelligence interest to the government. . . . The NSA could readily configure its surveillance equipment to ignore that traffic, or at least the significant portions of it (*e.g.*, Netflix traffic) that are almost certainly of no interest. Because of the substantial efficiency gains to be had, it is extremely likely that the government engages in this kind of filtering. . . .

Am. Compl. ¶ 59. If, as Plaintiff suggests, the NSA could choose to avoid wasting finite resources processing Netflix traffic, based on an assessment of its foreign-intelligence value, then the NSA similarly could choose not to use its limited surveillance resources to intercept, copy, or review information about the Wikimedia websites that users view online.

The degree to which Plaintiff encrypts its communications (and by what means) is also relevant to Plaintiff's standing. As noted above, Internet communications are encrypted specifically with the intent of preventing any party that might intercept them in transit from discerning their contents. If the NSA has not devised a way to break the encryption applied to a particular category of communications—again, whether and to what extent the NSA possesses such abilities, or does not, are classified facts—then devices used in connection with Upstream surveillance might be programmed to avoid alleged interception, copying, and review of those communications, including Plaintiff's, because effectively they would have no foreign-intelligence value. Thus, the extent to which Plaintiff's communications are encrypted, and how, whether using the HTTPS protocol or otherwise, are both relevant, because it is not the case that the NSA "must be" intercepting, copying, and reviewing communications of that kind.

Also relevant to jurisdiction is a breakdown of the volumes of each category of Wikimedia communications that Plaintiff contends is subjected to Upstream surveillance, and the countries to and from which communications in each category are sent. As the Fourth Circuit held, Plaintiff's standing is also premised, in part, on the idea that its communications are so numerous and geographically diverse that they must traverse "every international backbone link connecting the United States with the rest of the world." *Wikimedia*, 857 F.3d at 210; Am. Compl. ¶ 61. Plaintiff cannot establish its standing as to any of its identified categories of communications that does not meet these criteria of numerosity, and worldwide distribution. The information sought by the Government concerning the volume and distribution of Plaintiff's communications is therefore plainly relevant to the jurisdictional issue.

In sum, Plaintiff alleges it has standing to challenge Upstream surveillance on the theory that its Internet communications "must be" intercepted, copied, and reviewed as part of this surveillance. The Government is seeking basic technical information about Plaintiff's communications that its outside expert has determined, for the reasons explained above, is pertinent to evaluating the validity of that theory. This information is thus plainly relevant, and falls squarely within the scope of jurisdictional discovery authorized by the Court.

II. The Government's Discovery Requests Are Proportional to the Needs of the Case and Are Neither Overbroad, Unduly Burdensome, Nor Otherwise Improper.

Plaintiff also has failed to meet its burden of presenting particularized facts demonstrating that the Government's discovery requests are otherwise inappropriate. "[A] party objecting to a document request must specifically show how the request is burdensome, overly broad, [or] vague." *Haynes v. Navy Fed. Credit Union*, 286 F.R.D. 33, 36 (D.D.C. 2012); *see also Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 358 (D. Md. 2008) ("[B]oilerplate objections that a request for discovery is overboard and unduly burdensome . . . are improper

unless based on particularized facts." (citations omitted)). Here, Plaintiff's rote objections plainly fail to carry its burden.

Moreover, the Government's discovery requests are entirely appropriate. The Government's requests do not seek protocol, IP address, and encryption information about all Wikimedia communications, but only "each category of Wikimedia, international, text-based, Internet communications that Plaintiff contends, for purposes of establishing jurisdiction, is intercepted, copied, or reviewed by the NSA in the course of Upstream surveillance." *See* Ex. 1, Pl.'s Resp. to ODNI Interrogatory No. 19, at 8. The same is true of the Government's requests for information about the volume and distribution of Plaintiff's communications. The Government is only seeking information about categories of communications that Plaintiff intends to rely on to prove its standing—nothing else.[2] Without these additional facts, the Court may be presented with a skewed or incomplete picture about a central fact of this case: whether the technical rules governing how the Internet works require that Plaintiffs' communications "must be" subjected to Upstream surveillance. These requests are thus not overbroad and are proportional to the needs of this case.

Plaintiff has also provided no reason to believe that responding to these requests would be burdensome. Again, the Government is not asking Plaintiff to provide technical details and data about every type of communication in which it engages. Rather, the Government seeks only the facts about the categories of communications on which Plaintiff will rely to attempt to establish jurisdiction. Plaintiff has provided no explanation as to how this basic information could be difficult to assemble or otherwise be burdensome to set forth.

[2] Thus, contrary to Plaintiff's objections, ONDI Interrogatory No. 14 and DOJ Request for Production No. 1 are not "vague and ambiguous as to time." *See* Ex. 2, Pl.'s Resp. to ODNI's Second Set of Interrogatories, at 9–10; Ex. 3, Pl.'s Resp. to DOJ's First Set of Requests for Production, at 8. The applicable time period is the time period of the communications on which Plaintiff relies to attempt to prove its standing.

CONCLUSION

For the foregoing reasons, Plaintiff has failed to meet its burden of showing the Government's discovery requests seeking information regarding the protocols, IP addresses, and encryption of Plaintiff's Internet communications, and data about their volume and distribution, are improper. Therefore, Plaintiff should be directed to respond in full to ODNI Interrogatory No. 19, to ODNI Interrogatory No. 14 and to DOJ Request for Production No. 1, by June 1, 2018, or another reasonable date certain determined by the Court.

Dated: March 26, 2018

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTION
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
OLIVIA HUSSEY-SCOTT
Trial Attorneys

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Counsel for Defendants