

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 4/30/2020

----- X
:
THE NEW YORK TIMES COMPANY, et al., :
Plaintiffs, :
:
-against- :
:
THE FEDERAL COMMUNICATIONS :
COMMISSION, :
Defendant. :
----- X

18 Civ. 8607 (LGS)

OPINION AND ORDER

LORNA G. SCHOFIELD, District Judge:

Plaintiffs, The New York Times Company, Nicholas Confessore and Gabriel Dance (“NYT”), bring this action against Defendant, the Federal Communications Commission (“FCC”), seeking access to information in the FCC’s “API proxy server log” pursuant to the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552. Plaintiffs also seek the costs of this proceeding, including reasonable attorneys’ fees, under FOIA, 5 U.S.C. § 552(a)(4)(E). The parties cross-move for summary judgment. For the following reasons, Plaintiffs’ motion for summary judgment is granted, and Defendant’s motion is denied. Plaintiffs’ motion for reasonable attorneys’ fees is denied without prejudice to renew.

I. BACKGROUND

The facts in this background section are taken from the parties’ submissions and are undisputed. In May 2017, the FCC adopted a notice of proposed rulemaking with FCC Docket No. 17-108 titled “Restoring Internet Freedom.” The proposal sought to repeal rules enacted in 2015 governing internet service providers, popularly described as the rules that gave legal force to “net neutrality,” the principle that internet service providers must provide equal access to all web content regardless of the source. The proposal received substantial public attention. The

public was invited to submit comments to the FCC in the spring and summer of 2017 through the Commission’s Electronic Comment Filing System (“ECFS”), and over twenty million comments were submitted. The FCC enacted the proposed changes in December 2017, in effect repealing the so-called net neutrality rules. Since then, the press, academic researchers and governmental entities have investigated whether the public comment process was tainted by fraud, such as comments being submitted by automated bots and fraudulent email accounts. The existing research indicates that such concerns are not speculative or hypothetical. *See* Paul Hitlin and Skye Toor, *Public Comments to the Federal Communications Commission About Net Neutrality Contain Many Inaccuracies and Duplicates*, PEW RESEARCH CENTER (Nov. 29, 2017), <https://pewrsr.ch/2AiqeFR> (reporting that approximately 57% of the comments submitted included false or misleading personal information, that on nine different occasions, more than 75,000 comments were submitted at the very same second and that on at least five occasions, more than 24,000 exactly identical net neutrality comments were submitted to the FCC in a single second).

In June 2017, The New York Times submitted a FOIA request to the FCC for server logs related to public comments posted to FCC Docket No. 17-108 from April 2017 to June 2017. The request sought information that is automatically generated and transmitted to ECFS when comments are submitted. The New York Times and the FCC conferred for over thirteen months about the scope of the FOIA request. In August 2018, The New York Times submitted an amended request that sought only two types of data associated with comments submitted to ECFS regarding rulemaking No. 17-108 between April 26, 2017, and June 7, 2017:

- (1) “originating Internal Protocol (‘IP’) addresses” and related timestamps; and
- (2) “User-Agent headers” and related timestamps.

The FCC has a single “API proxy server log” that contains this

information, as well as other information. The New York Times has now agreed to narrow its request to entries in this log reflecting requests to submit comments (excluding requests to download comments), and as to those entries seeks only timestamps, originating IP addresses and User-Agent headers.

An IP address is a unique string of numbers that identifies each device on the internet. Every transaction over the internet transmits to the recipient the IP address of the transmitting computer. An originating IP address is defined in this case as the first IP address in the series of transmissions that occur when a comment is submitted to ECFS. In other words, this is the IP address for the device from which the ECFS comment was sent. Most consumer internet users get IP addresses for their devices on a dynamic basis from internet service providers. Dynamic IP addresses often change, and the FCC admits that “most users with dynamic IP addresses who submitted comments to ECFS in 2017 will likely have different IP addresses today.”

The User-Agent headers contain information about a commenter’s device, such as the operating system, operating system version, browser version, browser platform and language settings. This device-specific information can help distinguish between different users who share the same IP address.

When a comment is submitted to ECFS, the originating IP address and the User-Agent header data are automatically and necessarily transmitted to ECFS as well. The automatic transmission of this information is in contrast to the information that commenters must affirmatively include when filing a comment on ECFS -- the commenter’s name and postal address. Prior to filing a submission, the ECFS webpage displays a notice that states, “You are filing a document into an official FCC proceeding. All information submitted, including names and addresses, will be publicly available via the web.”

The New York Times received no response to the August 2018 request. Plaintiffs accordingly filed this action on September 20, 2018. Subsequently, the FCC issued a denial of The New York Times' administrative appeal. The agency stated that the requested information contained material that is exempt from disclosure pursuant to FOIA Exemptions 6 and 7(E), and that any non-exempt material could not be reasonably segregated and released. On this motion, the agency relies on FOIA Exemption 6.

II. STANDARD

“Summary judgment is the preferred procedural vehicle for resolving FOIA disputes.” *Nat'l Res. Def. Council v. U.S. Env'tl. Prot. Agency*, 403 F. Supp. 3d 270, 277 (S.D.N.Y. 2019); accord *White Coat Waste Project v. U.S. Department of Veterans Affairs*, 404 F. Supp. 3d 87, 95 (D.D.C. 2019) (“The ‘vast majority’ of FOIA cases can be resolved on summary judgment.”) (quoting *Brayton v. Office of the U.S. Trade Representative*, 641 F.3d 521, 527 (D.C. Cir. 2011)). When parties cross-move for summary judgment, the Court analyzes the motions separately, “in each case construing the evidence in the light most favorable to the non-moving party.” *Wandering Dago, Inc. v. Destito*, 879 F.3d 20, 30 (2d Cir. 2018). Summary judgment is appropriate where “there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” FED. R. CIV. P. 56(a). “A genuine issue of material fact exists if ‘the evidence is such that a reasonable jury could return a verdict for the nonmoving party.’” *Nick's Garage, Inc. v. Progressive Cas. Ins. Co.*, 875 F.3d 107, 113 (2d Cir. 2017) (quoting *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)).

“[A] district court must review *de novo* an agency's determination to withhold information requested under FOIA.” *Florez v. C.I.A.*, 829 F.3d 178, 182 (2d Cir. 2016); accord *Knight First Amendment Inst. at Columbia Univ. v. U.S. Dep't of Homeland Sec.*, 407 F. Supp.

3d 334, 328 (S.D.N.Y. 2019). “An agency withholding documents responsive to a FOIA request bears the burden of proving the applicability of claimed exemptions.” *Am. Civil Liberties Union v. U.S. Dep’t of Justice*, 681 F.3d 61, 69 (2d Cir. 2012). An agency may carry its burden by submitting affidavits or declarations, which must be “accorded a presumption of good faith.” *Florez*, 829 F.3d at 182. “FOIA exemptions are to be construed narrowly,” and there is a “strong presumption in favor of disclosure.” *Assoc. Press v. U.S. Dep’t of Def.*, 554 F.3d 274, 283 (2d Cir. 2009).

III. DISCUSSION

The FCC opposes disclosure of the requested material in the API proxy server log for two reasons. First, they contend that the requested information -- originating IP addresses and User-Agent headers -- is exempt from disclosure pursuant to FOIA Exemption 6. Second, they contend that because producing the requested information is unreasonably burdensome and unreliable, FOIA does not require compliance.¹

A. Exemption 6

FOIA requires federal agencies to make records available to the public unless a statutory exemption applies. *See* 5 U.S.C. § 552(a)(3)(A), (b)(1)-(9). FOIA Exemption 6 states that an agency may withhold “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(6). The Supreme Court has “regularly referred to [Exemption 6] as involving an ‘individual’s right to privacy.’” *FCC v. AT&T Inc.*, 562 U.S. 397, 408 (2011) (quoting *Dep’t of State v. Ray*, 502 U.S. 164, 175 (1991)).

¹ Prior to discovering the API proxy server log, the FCC also argued that Plaintiffs’ FOIA request required the agency to create new records. This argument was abandoned after the agency discovered the API proxy server log.

Courts “employ a two-prong inquiry in deciding whether the government has correctly withheld records under Exemption 6.” *Cook v. Nat’l Archives & Records Admin.*, 758 F.3d 168, 174 (2d Cir. 2014). The first prong is “whether the records in question are ‘personnel,’ ‘medical,’ or ‘similar’ files.” *Id.* “[T]he phrase ‘similar files’ [is meant] to have a broad, rather than a narrow, meaning.” *U.S. Dep’t of State v. Washington Post Co.*, 456 U.S. 595, 600 (1982). “[T]he Second Circuit considers ‘a record . . . a “similar file” if it contains personal information identifiable to a particular person.’” *Osen LLC v. United States Central Command*, 375 F. Supp. 3d 409, 423 (S.D.N.Y. 2019) (quoting *Cook*, 758 F.3d at 175). This “expansive interpretation . . . also encompasses bits of personal information that refer to a particular individual.” *Willis v. Federal Bureau of Investigation*, No. 17 Civ. 1959, 2019 WL 2138036, at *7 (D.D.C. May 16, 2019) (internal quotation omitted). If this step is met, the court undertakes a balancing inquiry. *See Cook*, 758 F.3d at 174.

“The first step in the balancing inquiry is determining whether disclosure ‘would compromise a substantial, as opposed to *de minimis*, privacy interest,’ because in the latter case, FOIA demands disclosure.” *Kuzma v. U.S. Dep’t of Justice*, 692 F. App’x 30, 34 (2d Cir. 2017) (summary order) (quoting *Cook*, 758 F.3d at 176); *see also White Coat Waste Project*, 404 F. Supp. 3d at 102 (“Substantial, in this context, means less than it might seem. A substantial privacy interest is anything greater than a *de minimis* privacy interest.”) (internal quotation marks omitted). “[T]he privacy side of the balancing test is broad and encompasses all interest involving the individual’s control of information concerning his or her person.” *Kuzma*, 692 F. App’x at 34 (quoting *Wood v. FBI*, 432 F.3d 78, 88 (2d Cir. 2005)) (internal quotation marks omitted). “[E]ven though ‘an event is not wholly private it does not mean that an individual has no interest in limiting disclosure or dissemination of the information.’” *Tomscha v. Gen. Servs.*

Admin., 158 F. App'x 329, 330 (2d Cir. 2005) (summary order) (quoting *Fed. Labor Relations Auth. v. U.S. Dep't of Veterans Affairs*, 958 F.2d 503, 510 (2d Cir. 1992)). “[R]egardless of the nature of the information contained in them, disclosure of records containing personal details about private citizens can infringe significant privacy interests.” *Cook*, 758 F.3d at 176 (quoting *Veterans Affairs*, 958 F.2d at 510) (internal quotation marks omitted). However, purely hypothetical or speculative privacy invasions are not considered, as the statutory text “refers to disclosures that ‘would constitute’ an invasion of privacy.” *Nat’l Archives & Records Admin. v. Favish*, 541 U.S. 157, 166 (2004) (comparing the text of Exemption 6 to Exemption 7(C), which broadly “encompasses any disclosure that ‘could reasonably be expected to constitute’ such an invasion”).

If a substantial privacy interest exists, the Court “consider[s] ‘the extent to which disclosure would serve the core purpose of FOIA,’ which is ‘contributing significantly to public understanding of the operations or activities of the government.’” *Cook*, 758 F.3d at 177 (quoting *U.S. Dep’t of Defense v. Fed. Labor Relations Auth.*, 510 U.S. 487, 495 (1994)) (emphasis in original). “[G]oals other than opening agency action to public scrutiny are deemed unfit to be accommodated under FOIA when they clash with privacy rights.” *Id.* (quoting *Veterans Affairs*, 958 F.2d at 510–11); see also *Pavement Coatings Tech. Council v. United States Geological Survey*, No. 14 Civ. 1200, 2019 WL 7037527, at *10 (D.D.C. Dec. 19, 2019) (“[D]isclosure must serve ‘the citizens’ right to be informed about what their government is up to”) (quoting *Beck v. Dep’t of Justice*, 997 F.2d 1489, 1491 (D.C. Cir. 1993)).

After identifying the cognizable privacy and public interests in the information, the Court balances them to determine whether disclosure “would constitute a clearly unwarranted invasion of personal privacy” in light of the public interest in the information. 5 U.S.C. § 552(b)(6).

1. Personnel, Medical or Similar Files

Under FOIA Exemption 6, an agency may withhold “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(6). Originating IP addresses and User-Agent header data are “similar files” for Exemption 6 purposes, and Plaintiffs do not dispute this conclusion. Data that provides information about a particular person without revealing his or her complete identity can qualify for Exemption 6 balancing. *See Hall v. C.I.A.*, 881 F. Supp. 2d 38, 71 (D.D.C. 2012). For example, a person’s date of birth, place of birth, social security number, blood type, place of residence, names of family members and religious affiliation are “similar files” protected under Exemption 6, *see id.*, as are email addresses. *See Prechtel v. Federal Commc’ns Comm’n*, 330 F. Supp. 3d 320, 329 (D.D.C. 2018). Because “similar files” has a “broad, rather than a narrow, meaning,” *Washington Post Co.*, 456 U.S. at 600, the data here meets the requirement, and the Court next undertakes the balancing inquiry.

2. Balancing Test

a. Privacy Interest

Whether disclosing IP addresses and device-specific information compromises a substantial privacy interest under Exemption 6 appears to be a question of first impression. *Cf.*, *Acosta v. F.B.I.*, 946 F. Supp. 2d 53, 63–65 (D.D.C. 2013) (under Exemption 7(C), agency is not required to disclose “IP addresses and other identifying computer information”); *Kortlander v. Bureau of Land Mgmt.*, 816 F. Supp. 2d 1001, 1014 (D. Mont. 2011) (same); *see also* 5 U.S.C. § 552(b)(7)(C) (Exemption 7(C) permits withholding “records or information compiled for law enforcement purposes” that “could reasonably be expected to constitute an unwarranted invasion of personal privacy.”). The question is extremely close in this case. Given this, the Court

assumes for purposes of the balancing analysis, but does not find, that disclosure of the IP addresses and User-Agent headers in the API proxy server log “would compromise a substantial, as opposed to *de minimis*, privacy interest.” See *Kuzma*, 692 F. App’x at 34 (quoting *Cook*, 758 F.3d at 176) (internal quotation marks omitted).

The strongest argument for finding a *de minimis* privacy interest is that the individuals who submitted FCC comments did so voluntarily, on a public website, providing their names and addresses along with their comments. A person’s name coupled with his address is the ultimate personal identifying information, as compared with a phone number or even an IP address, for example, which provides only a number associated with a device. Every commenter was provided with a privacy notice, stating that “[a]ll information submitted, including names and addresses, will be publicly available via the web.” Commenters arguably consented to the release of their IP addresses and other device-specific information, even though they may not have realized that the information was being divulged.

On the other hand, the strongest argument in favor of finding a substantial privacy interest is that digital advertisers and digital platforms could combine this data with other available information to create a detailed and intimate profile that might include information about a person’s race or ethnicity, political affiliation, religious belief, sexual identity and activity, income level, purchasing habits and medical information.² In other words, even though

² Defendant explains that “[t]hrough a process sometimes called ‘identity resolution,’ digital advertisers combine IP addresses, browser information, and other digital identifiers with more traditional off-line identification information (such as names, addresses, etc.) to create detailed profiles of individual consumers.” No. 18 Civ. 8607, ECF No. 24 ¶ 35. See also Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELECTRONIC FRONTIER FOUNDATION (Dec. 2 2019), <https://www.eff.org/wp/behind-the-one-way-mirror> (“The most prevalent threat to our privacy is the slow, steady, relentless accumulation of relatively mundane data points about how we live

IP addresses and other device-specific information do not themselves disclose a person's identity or any other identifying information, they can be used to help piece together other information and associate it with a particular person.

If the record provided further insight into how likely it is that this risk would materialize, then the agency might have sustained its burden of showing that the disclosure of IP addresses and User-Agent headers would compromise a substantial privacy interest. But the general statements in the agency's declaration that IP addresses and other digital identifiers "often can be reliably linked to individual persons" to create "detailed profiles" fall short. *See* No. 18 Civ. 8607, ECF No. 24 ¶ 35.³

Although the Court could grant Plaintiff's motion on this basis alone, the Court is reluctant to find on a less than developed record that the disclosure of IP addresses and User-Agent headers would affect only a *de minimis* privacy interest. In addition, the public interest in disclosure is sufficiently important here that it merits discussion, regardless of how the privacy interest is characterized.

b. Public Interest

On the other side of the balance, the Court considers the public interest in disclosure, specifically "the extent to which disclosure would serve the core purpose of FOIA, which is contributing significantly to public understanding of the operations or activities of the

our lives. . . . Trackers assemble data about our clicks, impressions, taps, and movement into sprawling *behavioral profiles*, which can reveal political affiliation, religious belief, sexual identity and activity, race and ethnicity, education level, income bracket, purchasing habits, and physical and mental health.").

³ Plaintiffs represent that its proposed statistical analysis of the data is "primarily geared at deducing broad patterns in the comments and the commenters' IP addresses and User-Agent information. It does not depend at all on the ability to match comments to IP addresses." No. 18 Civ. 8607, ECF No. 28 at 12 n.9.

government.” *Cook*, 758 F.3d at 177 (internal quotation marks and emphasis omitted). Here, disclosing the originating IP addresses and User-Agent headers would help clarify whether and to what extent fraudulent activity interfered with the comment process for the FCC’s rulemaking No. 17-108, and more generally, the extent to which administrative rulemaking may be vulnerable to corruption. This serves a vital public interest because of the importance of public comments in agency rulemaking.

The comment process is a critical part of administrative rulemaking, which is itself central to the operations and activities of government agencies. The FCC has been delegated authority to regulate interstate and international communications through rulemaking and other mechanisms. *See* 47 U.S.C. § 151, *et seq.* The Administrative Procedure Act requires that when an agency regulates through rulemaking, it must include a notice-and-comment process, providing interested persons “an opportunity to participate in the rule making through submission of written data, views, or arguments.” 5 U.S.C. § 553(c); *see also National Lifeline Assoc. v. Federal Commc’ns Comm’n*, 921 F.3d 1102, 1115 (D.C. Cir. 2019). The agency must then “consider[] . . . the relevant matter presented [and] . . . shall incorporate in the rules adopted a concise general statement of their basis and purpose.” 5 U.S.C. § 553(c). The comment process is sufficiently important that a rule may be vacated if the agency does not comply with the notice-and-comment requirements. *See, e.g., Am. Great Lakes Ports Ass’n v. Zukunft*, 296 F. Supp. 3d 27, 46, 56 (D.D.C. 2017) (holding that an agency’s compensation adjustment was arbitrary and capricious in part because it did not take into consideration comments, and noting that “[t]he typical remedy for arbitrary and capricious agency action is to vacate the rule”).

The integrity of the notice-and-comment process is directly tied to the legitimacy of an agency’s rulemaking. “Public oversight of agency action in the rulemaking context serves a

critical public function by protecting against agency overreaching and abuse of discretion.”⁴

All. for Wild Rockies v. Dep’t of Interior, 53 F. Supp. 2d 32, 37 (D.D.C. 1999); *see also F.C.C. v. Fox Television Stations, Inc.*, 556 U.S. 502, 537 (2009) (“Congress passed the Administrative Procedure Act (APA) to ensure that agencies follow constraints even as they exercise their powers.”). The notice-and-comment process is therefore central to the FCC’s operations of making rules that regulate communications.

In this case, the public interest in disclosure is great because the importance of the comment process to agency rulemaking is great. If “[t]he opportunity to comment is meaningless unless the agency responds to significant points raised by the public,” *United States v. Lott*, 750 F.3d 214, 219 (2d Cir. 2014) (quoting *Sherley v. Sebelius*, 689 F.3d at 784 (D.C. Cir. 2012)) (internal quotation marks omitted), then an agency must be able to discern what points are raised by the public. If genuine public comment is drowned out by a fraudulent facsimile, then the notice-and-comment process has failed. Disclosing the requested data in this case informs the public understanding of the operations and activities of government in two ways -- at the micro level with regard to the integrity of the FCC’s repeal of the particular net neutrality rules at issue, and at the macro level with regard to the vulnerability of agency rulemaking in general.⁵

⁴ The harms to public participation involved in “e-rulemaking” are not new. *See* Beth Simon Noveck, *The Electronic Revolution in Rulemaking*, 53 EMORY L.J. 433, 441–42 (Spring 2004) (“Increased network effects may not improve the legitimacy of public participation. For without the concomitant processes to coordinate participation, quality input will be lost; malicious, irrelevant material will rise to the surface, and information will not reach those who need it. In short, e-rulemaking will frustrate the goals of citizen participation.”). Relatedly, the E-Government Act of 2002 directs that all agencies must accept public comments on proposed rules electronically. *See* E-Government Act of 2002, Pub. L. No. 107-347, December 17, 2002, 116 Stat. 2899.

⁵ The E-Government Act recognizes that “[t]he use of computers and the Internet is rapidly transforming societal interactions and the relationships among citizens, private businesses, and

The FCC contends that even if disclosure serves a public interest, that interest is diminished because of alternative sources of similar information, for example, other ongoing public and private investigations into the bona fides of the public comment process for rulemaking No. 17-108. But the FCC does not assert that these investigations would reveal the same information that Plaintiffs seek here, or reveal the FCC's operations and activities in the same way as the information Plaintiffs request. Even if the other sources were adequate alternatives, this is just "one factor" for courts to consider, and given the weighty public interest already discussed, it is not a strong factor here. *U.S. Dep't of Def. v. Fed. Labor Rel. Auth.*, 964 F.2d 26, 29 (D.C. Cir. 1992).

The FCC also argues that adequate information is already available to the public to assess the agency's operations and activities. The agency notes that its final rule runs over 500 pages and describes the public comments and other sources considered. This misunderstands the public interest at stake. The concern is not whether the FCC was appropriately responsive to certain comments. Rather, the concern is whether the notice-and-comment process functioned as a check on agency rulemaking authority as prescribed by federal administrative law.

c. Balancing

FOIA Exemption 6 prohibits disclosure only when doing so "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). "FOIA exemptions are to be construed narrowly," and there is a "strong presumption in favor of disclosure." *Assoc. Press*, 554 F.3d at 283. Weighing the private and public interests as discussed above, and in light of the "strong presumption in favor of disclosure," Exemption 6 does not shield from disclosure the

the Government." *Id.* at § 2(a)(1). It goes without saying that the use of computers and the internet has substantially increased since the Act was passed in 2002.

requested IP addresses and User-Agent fields in the API proxy server log in this case. *Assoc. Press*, 554 F.3d at 283.

B. Defenses to Production

The FCC contends that because producing the requested information is unreasonably burdensome and unreliable, FOIA does not require compliance. FOIA requires that agencies “upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules . . . [,] make the records promptly available to any person.” 5 U.S.C. § 552(a)(3)(A). “Agencies responding to such record requests must “make *reasonable efforts to search* for the [requested] records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency’s automated information system.” 5 U.S.C. § 552(a)(3)(C) (emphasis added). “[S]earch’ means to review, manually *or by automated means*, agency records *for the purpose of locating those records* which are responsive to the request.” 5 U.S.C. § 552(a)(3)(D) (emphasis added). “Record” is defined to include “information that would be an agency record subject to the requirements of this section when maintained by an agency *in any format, including an electronic format.*” 5 U.S.C. § 552(f)(2)(A) (emphasis added). None of the agency’s defenses to production are persuasive.

First, the FCC contends that the API proxy server log is not actually a database, but instead “a long and unwieldy list of various data” that it should not have to search. The agency does not address why such a list does not fall under “information . . . in any format” that is subject to FOIA. *Id.* Other courts have acknowledged that similar data logs can be subject to FOIA. *See, e.g., Prechtel*, 330 F. Supp. 3d at 333–34 (noting that FOIA likely would require the disclosure of .CSV files, which are “essentially . . . spreadsheet[s] in which every row contains a separate comment” if the FCC maintains the files); *Inst. for Justice v. Internal Revenue Serv.*,

941 F.3d 567, 568–69, 571 (D.C. Cir. 2019) (noting that the term “database . . . has no independent legal significance under FOIA” and means simply “a system that stores and contains records subject to FOIA”).

Second, the FCC objects to producing the relevant materials from the API proxy server log because to do so requires creating a script, which demands “research” rather than simply a “search.” This argument also fails as a matter of law. In contrast to completing a “search,” which FOIA defines as reviewing agency records by automated means to locate responsive records, *see* 5 U.S.C. § 552(a)(3)(D), conducting research and answering questions require “dig[ging] out all the information that might exist, in whatever form or place it might be found.” *See Tokar v. U.S. Dep’t of Justice*, 304 F. Supp. 3d 81, 91 (D.D.C. 2018). The FCC contends that the purpose of the script is to conduct a “matching and sorting process” that pulls only the relevant material from the API proxy server log. This “matching and sorting” process is closer to an automated search for responsive records than a scavenger hunt for disparate information. FOIA “clearly require[s] agencies to sort a pre-existing database of information to make information intelligible so that it may be transmitted to the public.” *Everytown for Gun Safety Support Fund v. Bureau of Alcohol, Tobacco, Firearms & Explosives*, 403 F. Supp. 3d 355, 356 (S.D.N.Y. 2019) (internal quotation marks omitted). “Accordingly, conducting such a search cannot constitute . . . conducting research so as to fall outside of agency disclosure requirements.” *Id.*

In addition, the FCC has made no showing that creating and running such a script would require more than “reasonable efforts to search” or “would significantly interfere with the operation of the agency’s automated information system.” 5 U.S.C. § 552(a)(3)(C); *see Pinson v. Dep’t of Justice*, 80 F. Supp. 3d 211, 216 (D.D.C. 2015) (noting that courts “often look for a

detailed explanation by the agency regarding the time and expense of a proposed search in order to assess its reasonableness” (internal quotation mark omitted)).⁶

Finally, the FCC contends that the script will not precisely extract information associated with rulemaking No. 17-108, such that the results will be unreliable. Plaintiffs suggest that less than 0.7% of the entries submitted on ECFS during the relevant time period were unrelated to rulemaking No. 17-108. Defendants similarly state that over 99% of comments submitted during that time period relate to rulemaking No. 17-108. Accordingly, the risk of producing inaccurate information is insufficient to overcome the “strong presumption in favor of disclosure.” *Assoc. Press*, 554 F.3d at 283.

C. Reasonable Attorneys’ Fees

“Under 5 U.S.C. § 552(A)(4)(E)(i), the Court may assess reasonable attorney fees and other litigation costs reasonably incurred by a FOIA plaintiff that has substantially prevailed. The test for an award of fees has two components: eligibility and entitlement.” *Am. Oversight v. U.S. Dep’t of Justice*, 375 F. Supp. 3d 50, 60–61 (D.D.C. 2019) (alterations added and internal citation omitted). “The eligibility prong asks whether a plaintiff has ‘substantially prevailed’ and thus ‘may’ receive fees.” *Id.* at 61 (quoting *Brayton*, 641 F.3d at 524) (internal quotation marks omitted). “If so, the court proceeds to the entitlement prong and considers a variety of factors to determine whether the plaintiff *should* receive fees.” *Id.* (quoting *Brayton*, 641 F.3d at 524) (internal quotation marks omitted). The parties have not briefed this issue. Accordingly, Plaintiffs’ motion for reasonable attorneys’ fees and other litigation costs is denied without prejudice to renew the request.

⁶ Because the agency has not established that the burden of producing just the requested information exceeds “reasonable efforts,” this opinion does not address the FCC’s objection to producing the entire API proxy server log.

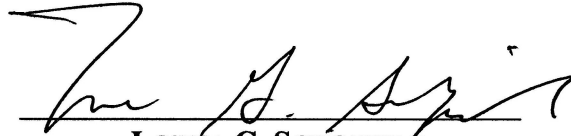
IV. CONCLUSION

For the foregoing reasons, Plaintiffs' motion for summary judgment is GRANTED, and Defendant's motion for summary judgment is DENIED. Plaintiffs' motion for reasonable attorneys' fees is DENIED without prejudice to renew.

The Clerk of Court is respectfully directed to close the motions at Docket Nos. 22 and 27.

SO ORDERED.

Dated: April 30, 2020
New York, New York



LORNA G. SCHOFIELD
UNITED STATES DISTRICT JUDGE