Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matters of	)	
	)	
Nicholas Confessore	)	FOIA Control No. 2017-764
	)	
Jeremy Singer-Vine	)	FOIA Control No. 2018-204
	)	
On Request for Inspection of Records	)	

MEMORANDUM OPINION AND ORDER

Adopted: November 7, 2018 **Released: December 3, 2018**

By the Commission: Chairman Pai issuing a statement; Commissioner Rosenworcel dissenting and issuing a statement.

I. INTRODUCTION

1. The Freedom of Information Act (FOIA) provides the public with access to agency records. Although the FOIA generally requires the disclosure of agency records, it provides nine exemptions to protect those records that would not be suitable for release to the public. Among other things, those exemptions permit withholding of material that would disclose certain private information (Exemption 6) or particular information related to law enforcement and security matters (Exemption 7). Here, Nicholas Confessore[1] and Jeremy Singer-Vine[2] challenge the application of those exemptions to FOIA requests they filed for portions of the Commission's server logs for the Electronic Comment Filing System (ECFS) related to Docket No. 17-108. Shortly before our decision today, in *Prechtel v. Federal Communications Commission*,[3] the United States District Court for the District of Columbia held that essentially the same server logs were exempt from disclosure under the FOIA pursuant to Exemption 7. For the reasons stated in that opinion, and for the further reasons set forth herein, we deny Confessore and Singer-Vine's applications for review, concluding that staff in the Office of the Chief Information Officer properly withheld this information.

II. BACKGROUND

2. *Confessore Request – FOIA 2017-764.* Confessore, on behalf of the New York Times, filed a FOIA request seeking "web server logs for comments submitted for Federal Communications Commission docket No. 17-108 between 4/26/17 and 6/7/17."[4] He requested that the Commission provide certain technical information for each comment in the docket, including the IP address of the client making the request.[5]

[1] Letter from Ian MacDougall, Legal Counsel, New York Times, to Appeals Officer, Federal Communication Commission (July 25, 2017) (2017-764 Initial Appeal).

[2] Letter from Jeremy Singer-Vine, Buzzfeed News, to Federal Communications Commission (February 26, 2018) (2018-204 Appeal).

[3] Case No. 17-cv-01835 (CRC), 2018 WL 4374924 (D.D.C. Sept. 13, 2018).

[4] Nicholas Confessore, FOIAonline Request, 2018-764 (June 22, 2017) (2017-764 Initial Request).

[5] *Id.*

3. Staff responded to Confessore's request, stating that all records were being withheld in full under FOIA Exemption 6, which protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy if released.[6] Staff concluded that the requested records consisted of non-public information of the ECFS commenters and thus that they should be withheld under Exemption 6.[7] Office of General Counsel staff subsequently supplemented that response, providing additional information as to why the records could not be disclosed.[8] The supplemental response reiterated the applicability of Exemption 6, emphasizing that IP addresses requested by Confessore were private information that could be linked back to the individual commenters.[9]

4. Additionally, the supplemental response explained that the records had been withheld under Exemption 7(E), which protects "records or information compiled for law enforcement purposes [the production of which] would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk a circumvention of the law."[10] In particular, the supplemental response stated that disclosure of the logs "would provide detailed information about the Commission's relationship with commercial cloud servers and the infrastructure the Commission uses to manage ECFS and protect it from disruptive attacks . . . [and] detailed information about the steps the FCC took in response to the spike in ECFS traffic during early May [2017]." This information "could reasonably be expected to risk a circumvention of the law" because it would "giv[e] future attackers a 'roadmap' to evade the Commission's future defensive efforts."[11]

5. To the extent that Confessore requested any information that was not exempt from disclosure under the FOIA, the supplemental response went on to explain that such information could not be reasonably segregated out for disclosure, because it was inextricably intertwined with exempt information.[12] The response further explained that the requested server logs are comprised of millions of lines of technical information, and the process of redacting out commenters' IP addresses and sensitive security information would require an "inordinately burdensome" review process.[13]

6. Confessore appeals both the initial and supplemental responses.[14] Confessore contends that Exemption 6 could not be used to withhold the IP addresses in question. First, he argues that the statutory text of Exemption 6 limits its protection to "personnel and medical files and similar files."[15] Confessore contends that the IP addresses are not contained in anything resembling a personnel or medical file, and thus they cannot be withheld under Exemption 6.

7. Second, Confessore insists that the ECFS comment guide notifies commenters that "[a]ny comments that you submit to the FCC . . . will be made public, including any personally identifiable

[6] Letter from Christine Calvosa, Deputy Chief Information Officer, Federal Communications Commission, to Nicholas Confessore (July 21, 2017) (July 21, 2017) (2017-764 Initial Decision).

[7] *Id.*

[8] Letter from John Williams, Senior Counselor, Office of General Counsel, FCC to Christina Koningisor, Legal Department, New York Times (Jan. 29, 2018) (2017-764 Supplemental Response).

[9] *Id.* at 1-2.

[10] *Id.* at 2-3; 5 U.S.C. § 552(b)(7)(E).

[11] 2017-764 Supplemental Response at 3.

[12] *Id.* at 3.

[13] *Id.* at 4.

[14] 2017-764 Initial Appeal; Letter from Christina Koningisor, Legal Department, New York Times (Feb. 26, 2018) (2017-764 Supplemental Appeal).

[15] 2017-764 Initial Appeal at 2 (quoting 5 U.S.C. § 552(b)(6)); 2017-764 Supplemental Appeal at 3.

information you include in your submission."[16] Confessore notes that the ECFS filing system provides a similar notice to commenters, stating, "All information submitted, including names and addresses, will be publicly available via the web."[17] Based on these representations, Confessore asserts that commenters have waived their privacy interests in their IP addresses when they submit a comment on ECFS. To the extent that such information would otherwise be protected under Exemption 6, Confessore contends that the personal privacy interest in the information is *de minimis*, while the public interest in understanding the origin of the comments filed in Docket No. 17-108 is strong.[18]

8. Confessore also disputes the withholding of records under Exemption 7(E). He first argues that the logs themselves are not tied to any investigation or prosecution, and thus that the logs fail to satisfy a threshold requirement of Exemption 7(E).[19] Second, Confessore states that, based on discussions between Commission staff and the New York Times, he had narrowed his request to just four technical pieces of information, including IP addresses.[20] He contends that this narrowing should be sufficient to eliminate any security concerns.[21]

9. On the issue of segregating non-exempt information, Confessore states that his prior narrowing should reduce the scope of his request to only non-exempt information.[22] He further states that the Commission should be able to extract the requested non-exempt information without the need for line-by-line review of the ECFS server logs.[23] While his appeal was pending, Confessore also offered to modify his request, asking the Commission to produce two sets of logs.[24] The first set would indicate the IP address from which the requests originated while the second set would include other information about the computer systems from which the requests originated.[25] Confessore proposed that the Commission could link the two sets of logs by creating a unique identifier, thereby associating each entry in the two sets of logs.

10. *Singer-Vine Request – FOIA 2018-204.* Singer-Vine, on behalf of Buzzfeed News, filed a FOIA request seeking "server logs corresponding to the submissions of . . . 20 ECFS filings responding to Proceeding 17-108."[26] The request specified the particular data points Singer-Vine sought, including the IP address from which the filings originated.[27] Singer-Vine claimed that these IP addresses were not subject to protection under Exemption 6 because, he believed, "the submissions were 'faked,' i.e., submitted by a computer program using names, email addresses, and physical addresses stolen from

[16] 2017-764 Initial Appeal at 2; 2017-764 Supplemental Appeal at 3.

[17] 2017-764 Initial Appeal at 2; 2017-764 Supplemental Appeal at 3-4.

[18] 2017-764 Supplemental Appeal at 4.

[19] *Id.* at 4-5.

[20] *Id.* at 2. The four pieces of information are X-Forward-For header, date/time stamp of each request, IP address of the client making the request, and browser USERAGENT.

[21] *Id.* at 5.

[22] *Id.* at 5.

[23] *Id.* at 5.

[24] Letter from Christina M. Koningisor, Legal Department, New York Times, to John Williams, Senior Counselor, Office of the General Counsel, FCC (May 7, 2018) (May 7 Letter). The request was further modified in a subsequent letter. Letter from Christina M. Koningisor, Legal Department, New York Times, to John Williams, Senior Counselor, Office of the General Counsel, FCC (August 31, 2018) (August 31 Letter).

[25] In particular, Confessore requested USERAGENT header information.

[26] Jeremy Singer-Vine, FOIAonline Request, 2018-204 (Dec. 6, 2017) (2018-204 Request). The request provided the submission ID for each of the twenty requests in question.

[27] *Id.*at 2.

hacked data," noting that the text matched the pattern of "faked" submissions, that all 20 comments were filed at the same time, and that the identities used appear to be linked to a prior data breach.[28]

11. Staff responded to Singer-Vine's request, stating that the records were being withheld in full under FOIA Exemption 7(E).[29] As in its supplemental response to Confessore's FOIA request, staff explained that disclosure of the logs would "publicly disclose information about how the FCC protects the security of ECFS and its other information assets," including information about the tools it uses to protect systems from disruptive attacks.[30]

12. Singer-Vine appeals the response to his request.[31] He argues that the server logs do not qualify for protection under Exemption 7(E), as the Commission has not demonstrated that they were compiled for law enforcement purposes.[32] Singer-Vine also claims that the Commission failed to show that the records were related to a "guideline, technique, or procedure" or that release of the records would risk circumvention of the law or that release would harm an interest protected by Exemption 7(E).[33] Lastly, Singer-Vine contends that the Commission has failed to show that non-exempt portions of the records could not be segregated out and produced to him.[34]

III. DISCUSSION

13. We affirm the staff decision that the server logs are exempt from disclosure under FOIA Exemption 6 and Exemption 7(E). We agree with the initial determination that there is no non-exempt portion of the records that can be reasonably segregated and produced to the requesters. Therefore, we conclude that the requested records may be withheld in full.

A. Exemption 6

14. We conclude that IP addresses contained within the server logs constitute private information that is exempt from FOIA disclosure under Exemption 6.

15. For a record to qualify for protection under Exemption 6, it must satisfy two elements. First, the record must consist of "personnel and medical files and similar files."[35] The U.S. Supreme Court has recognized that "the protection of Exemption 6 is not determined merely by the nature of the file in which the requested information is contained"[36] and accordingly interpreted Exemption 6's "similar files" language to encompass any "information which applies to a particular individual."[37] Second, the record must be such that "disclosure . . . would constitute a clearly unwarranted invasion of personal privacy."[38] Answering this question requires that we assess and balance the public's interest in disclosure

[28] *Id.* at 2-3.

[29] Letter from Christine Calvosa, Acting Chief Information Officer, Federal Communications Commission, to Jeremy Singer-Vine, Buzzfeed News (February 16, 2018) (2018-204 Response).

[30] *Id.* at 2. Staff stated that because the records could be withheld in full under Exemption 7(E), it did not address Singer-Vine's claims under Exemption 6.

[31] 2018-204 Appeal.

[32] *Id.* at 4.

[33] *Id.* at 3, 5-6.

[34] *Id.* at 6.

[35] 5 U.S.C. § 552(b)(6).

[36] *Id.* at 601.

[37] *Dep't of State v. Washington Post Co.*, 456 U.S. 595, 602 (1982).

[38] *Id.*

of this information against the individual's privacy interest in the confidentiality of this information.[39] We conclude that IP addresses of ECFS commenters contained in the server logs satisfy each of these elements.

16. We conclude that IP addresses meet the first element because they are contained in "similar files," as that term is used in the context of the FOIA.[40] As previously explained by Commission staff, the relevant inquiry is whether the IP addresses apply to a particular individual. Similar to a phone number or mailing address, an IP address can be linked, in conjunction with other information,[41] to a particular computer or individual.[42] Because the server logs contain IP addresses which can be linked to a particular individual, the server logs themselves fall within the "similar files" requirement, as set forth by the Supreme Court.

17. We disagree with Confessore, who argues that the IP addresses "[do] not reside in a file that resembles a personnel or medical file" and therefore do not qualify for protection under Exemption 6.[43] As explained, courts do not interpret Exemption 6 so narrowly; they have focused on the function of the exemption—protecting personal information—not other issues like the formatting of the files. Thus, the fact that the IP addresses are contained in server logs, as opposed to records more closely resembling personnel or medical files, is not determinative.[44]

18. We also conclude that the balance of interests weighs in favor of withholding the IP addresses and that releasing them would constitute "a clearly unwarranted invasion of personal privacy."

19. First, we conclude that individuals possess a substantial privacy interest in their IP addresses,[45] consistent with the findings of several federal courts.[46] In combination with other information, IP addresses can be traced back to a particular computer or individual. A given IP address

[39] *See, e.g.*, *Dep't of the Air Force v. Rose*, 425 U.S. 352, 372 (1976).

[40] We principally address Confessore's arguments regarding Exemption 6, as staff did not directly address Exemption 6 issues in its response to Singer-Vine. However, our reasoning applies equally to both appeals.

[41] For the FOIA privacy analysis, it is not necessary that the released records immediately and directly cause a harm to individuals' privacy interests. "Where there is a substantial probability that disclosure will cause an interference with personal privacy, it matters not that there may be two or three links in the causal chain." *Nat'l Ass'n of Retired Fed. Employees v. Horner*, 879 F.2d 873, 878 (D.C. Cir. 1989). *See also Nat'l Ass'n of Builders v. Norton*, 309 F.3d 26, 35 (D.C. Cir. 2002) (protecting square and lot numbers of properties as that information, combined with other publicly available records, could be used to identify the property owners).

[42] *See generally*, U.S. Computer Emergency Readiness Team, Department of Homeland Security, "Home Network Security," https://www.us-cert.gov/Home-Network-Security. We note that under the New York Times' own privacy policy, when IP addresses are combined with other personal information about consumers, the combined information is treated as personal information. New York Times, Privacy Policy, https://help.nytimes.com/hc/en-us/articles/115014892108-Privacy-policy (last visited Jul. 18, 2018).

[43] 2017-764 Appeal at 2.

[44] *See* 2017-764 Supplemental Response at 1.

[45] The Commission has publicly acknowledged that some of the comments made in ECFS during the period in question came from cloud-based automated "bots," but a large number came from human users who accessed the site to submit comments in the proceeding. *See, e.g.*, Letter from Ajit V. Pai, Chairman, Federal Communications Commission, to U.S. Senator Ron Wyden (June 15, 2017).

[46] This conclusion is consistent with the findings of district courts that have had opportunity to address the applicability of FOIA's privacy exemptions to IP addresses. *See Kortland v. BLM*, 816 F. Supp. 2d 1001, 1015 (D. Mont. 2011) (including IP addresses with names, addresses, and phone numbers as material suitable for withholding under Exemptions 6 and 7(C)); *Acosta v. FBI*, 946 F. Supp. 2d 53, 65 (D.D.C. 2013) (approving of redactions under Exemption 7(C), noting that the withholdings are "careful and pinpointed redactions of names, words, clauses, and sentences, including, for example, *pages that contain only IP addresses and other identifying computer information*.") (emphasis added).

may be associated with an individual over an extended period of time, persisting over multiple transactions on the Internet.[47] Thus, the same IP address that was used to file comments in ECFS could follow that user as she engaged in online banking, researched a medical condition, or checked the website of her child's school. Providing a list marrying each comment to a particular IP address would allow an individual to connect the IP address to a given name, mailing address, e-mail address, and other information provided by users in ECFS. This would make it substantially easier to link an otherwise anonymous IP address used across the Internet to a specific individual. Given these concerns, we conclude that there is a substantial privacy interest in the requested records.

20. Next, we find that Confessore has articulated a non-*de minimis* public interest in the release of these records. Specifically, Confessore contends there is a public interest in release of these records because they will reveal how "cloud-based automated bots are being used to influence an array of U.S. political activities—including the agency notice and comment process."[48]

21. Having concluded that there exists both a substantial private interest in preserving the confidentiality of the IP addresses and a public interest in understanding the operation of the comment process, we must balance these two competing interests against one another. In doing so, we conclude that the privacy interest considerably outweighs the public interest and that disclosure would constitute a clearly unwarranted invasion of personal privacy.

22. In weighing the public interest in this matter, we must consider whether the same public interest could be served through less intrusive means.[49] Confessore proffers a putative public interest in understanding the integrity of the Commission's comment process.[50] This question, however, is being or has already been examined by other press outlets,[51] Commission staff, and the Government Accountability Office, among others.[52] Confessore has not provided us with any reason to believe that his review of this data would significantly advance any public interest beyond the investigations that are already underway.[53] Relatedly, it is possible to meaningfully inform the public about these and similar matters without access to the sensitive server logs.[54] Therefore, we conclude that the privacy interest in protecting the personal information contained in the server logs substantially outweighs the marginal benefit to the public in disclosing the logs.

23. We disagree with Confessore's argument that we should ignore the privacy interest of these individuals because "individuals that choose to submit a comment to the FCC knowingly and

[47] This is especially true for users with a static IP address, but even dynamic IP addresses may continue to be associated with a single user for substantial periods of time. *See* U.S. Computer Emergency Readiness Team, Department of Homeland Security, "Home Network Security," https://www.us-cert.gov/Home-Network-Security.

[48] 2017-764 Supplemental Appeal at 4.

[49] *Dep't of Defense v. FLRA*, 964 F.2d 26, 29-30 (D.C. Cir. 1992) (noting that it is appropriate for an agency to consider "the extent to which there are alternative sources of information available that could serve the public interest in disclosure.")

[50] *See* 2017-764 Supplemental Appeal at 4.

[51] *See, e.g.*, James V. Grimaldi and Paul Overberg, "Millions of People Post Comments on Federal Regulations. Many Are Fake," *Wall Street Journal* (Dec. 12, 2017).

[52] *See, e.g.*, Letter from Orice Williams Brown, Managing Director of Congressional Relations, U.S. Government Accountability Office, to the Honorable Frank Pallone, Jr., Ranking Member, Committee on Energy and Commerce, U.S. House of Representatives (Jan. 9, 2018).

[53] *Cf. Nat'l Archives and Records Admin. v. Favish*, 541 U.S. 157, 175 (2004) (declining to find a public interest where multiple investigations had already examined a matter).

[54] *See, e.g.*, James V. Grimaldi & Paul Overberg, *Millions of People Post Comments on Federal Regulations. Many Are Fake.*, Wall St. J., Dec. 12, 2017; James V. Grimaldi and Paul Overberg, *The NFL's Other Problem: Fake Fans Lobbying for the Blackout*, Wall St. J., Sept. 7, 2018.

willingly waive whatever privacy interest they might otherwise have had."[55] Although ECFS's comment guide contains a disclaimer that "[a]ny comments that you submit to the FCC . . . will be made public, including any personally identifiable information you include in your submission,"[56] the disclaimer does not extend to IP addresses. For one, unlike a name or mailing address, the IP address is not affirmatively entered by the user, but rather is collected automatically as part of the necessary interaction between the user's computer and ECFS. Thus, it is not part of the "information *you include* in *your submission*." Indeed, many users may be unaware that IP addresses are exchanged when they submit their comments and that their IP addresses can be linked to their online activities unrelated to submitting comments to the FCC.[57] For another, ECFS does *not* make commenter IP addresses public. And accordingly, no commenter, in viewing other comments on ECFS as a basis for comparison, would reasonably believe his IP address would be made public, as that information is not included in the posted comments unlike other information included in a filer's submission. Indeed, Confessore's entire FOIA request is predicated on the fact that this information is not publicly available.

B. Exemption 7(E)

24. As a separate and independent ground for our decisions, we conclude the requested server logs are protected from disclosure under Exemption 7(E) —a determination that was essentially affirmed by a federal district court recently in connection with a similar request for the FCC's server logs.[58] An agency may withhold a record under Exemption 7(E) if the information contained therein is (1) "compiled for law enforcement purposes" and (2) release of the information "could reasonably be expected to risk circumvention of the law."[59] A record is considered to be "compiled for law enforcement purposes" if there is a rational nexus between the record and the agency's law enforcement or national security duties and there is a connection between an individual or incident and a possible security risk or violation of federal law.[60] Courts have often extended Exemption 7(E)'s ambit to include techniques or procedures aimed at the prevention of crimes and matters of general security.[61] Courts have also recognized that Exemption 7(E) creates "a relatively low bar for the agency [to meet] to justify withholding."[62]

25. We first conclude that the server logs in question have a rational nexus to the Commission's law enforcement functions. The Communications Act entrusts the Commission with numerous law enforcement and national security functions related to the nation's communications systems, including those functions carried out by the Commission's Enforcement Bureau and Public Safety and Homeland Security Bureau, and the Commission routinely coordinates with the Department of

[55] 2017-764 Supplemental Appeal at 3-4; 2017-764 Initial Appeal at 2.

[56] Federal Communications Commission, *How to Comment on FCC Proceedings* (Apr. 10, 2018) https://www.fcc.gov/consumers/guides/how-comment.

[57] *See supra* at para. 19.

[58] *See Prechtel* at *10-11.

[59] *Piper v. Dep't of Justice*, 294 F. Supp. 2d 16, 30 (D.D.C. 2003).

[60] *Ctr. for Nat'l Sec. Studies v. Dep't of Justice*, 331 F.3d 918, 926 (D.C. Cir. 2003).

[61] *Judicial Watch v. Dep't of Commerce*, 337 F. Supp. 2d 146, 181-82 (D.D.C. 2004) (applying Exemption 7(E) to withhold security procedures, firearm specifications, and radio frequencies, all used to protect the Secretary of Commerce); *Voinche v. FBI*, 940 F. Supp. 323, 332 (D.D.C. 1996) (applying Exemption 7(E) to withhold "information relating to an analysis of safety procedures afforded to the Supreme Court and its Justices"); *U.S. News & World Report v. Dep't of the Treasury,* No. 84-2303, 1986 U.S. Dist. LEXIS 27634, at *5 (D.D.C. Mar. 26, 1986) (applying Exemption 7(E) to withhold technical specifications of the presidential limousine).

[62] *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011).

Justice on the enforcement of federal communications laws.[63] Furthermore, the Commission's Office of the Inspector General is often involved in the investigation of potential criminal matters.[64] The Commission relies on a secure and robust IT system, including ECFS, to carry out these functions. The information contained in the ECFS server logs could be used to disrupt not only ECFS, but potentially more sensitive Commission systems that are directly relied on by the Commission in carrying out its law enforcement and national security functions. As such, the Commission's IT systems are a critical law enforcement tool, as the missions of the Enforcement Bureau, the Public Safety and Homeland Security Bureau, and the Office of the Inspector General would be severely hampered if the Commission's IT systems were unavailable or compromised. The server logs are just one component, compiled in support of that tool, and release of the logs could jeopardize the security of the IT system.[65]

26. We also find a connection between the disclosure of the security logs and a possible security risk or violation of law. The information contained in the server logs could be used by malicious actors to exploit vulnerabilities in the Commission's IT infrastructure and defeat countermeasures the Commission deploys to respond to attacks. This would threaten the Commission's ability to carry out its law enforcement and national security functions.[66] Therefore, we conclude that the server logs constitute records compiled for law enforcement purposes under the FOIA.

27. We next disagree with Confessore's argument that Exemption 7(E) should not apply because the server logs are not "tethered to a law enforcement 'investigation[] or prosecution[].'"[67] Exemption 7(E) does not require an agency to link the records to a specific investigation or prosecution.[68] The techniques the Commission employs to protect its IT infrastructure are intended to prevent certain computer-related crimes, such as the malicious disruption of government systems,[69] that might otherwise occur. Furthermore, revealing the server logs could impede future investigations into cyber incidents against the Commission by providing adversaries with a roadmap as to what attacks might escape detection. The logs provide details on the internal IT systems both in the aggregate and in particular, which contain data elements revealing systems structure and application design that can be mapped out. Disclosure of either of these could result in the discovery of potential attack vectors. The logs also contain information on the timing and nature of how the Commission deploys its tools to handle surges in web traffic. This information would provide malicious actors with insight into how the Commission protects its systems and would improve their ability to defeat those protections. The logs also contain information about the steps Commission staff took during the period in question, including alterations to ECFS's code and changes in how the system operated. The disclosure of this information could provide malicious actors with the insight to evade the Commission's defensive efforts going forward.

---

[63] *See, e.g.*, 47 U.S.C. § 151 (granting the Commission authority to "execute and enforce the provisions of this [Act]"); 47 U.S.C. § 401 (enforcement provisions); 47 U.S.C. § 615a-1 (certain 911 authorities of the Commission).

[64] 47 CFR § 0.13.

[65] For these reasons, we disagree with Confessore's contention that the Commission is not "involved in any 'law enforcement efforts'" that would justify invoking Exemption 7(E). 2017-764 Supplemental Appeal at 5.

[66] *See Levinthal v. Fed. Election Comm.*, 219 F. Supp. 3d 1, 6 (D.D.C. 2016) (withholding certain Federal Election Commission records regarding IT security).

[67] 2017-764 Supplemental Appeal at 4-5.

[68] *See Levinthal*, 219 F. Supp. 3d at 7 ("[Plaintiffs] contend that the NIST Study is not 'compiled for law enforcement purposes' because '[i]t is not connected to an investigation.' That argument misconstrues the law. The Court of Appeals consistently has held that records do not have to be linked to a specific investigation to be properly withheld under Exemption 7(E).") (internal citations omitted); *Gordon v. FBI*, 388 F. Supp. 2d 1028, 1036 (N.D. Cal. 2005) ("Exemption 7(E) is not limited to documents created in connection with a criminal investigation.").

[69] 18 U.S.C. § 1030.

28. Singer-Vine's argument that "the requested records simply do not qualify as guidelines, techniques, or procedures"[70] likewise falls short. For one, his assertion is just that—a mere assertion without explanation or analysis. For another, the information that can be gleaned from the records—the particular countermeasures and internal system architecture used to protect the Commission's IT infrastructure—fall within Singer-Vine's own definitions of techniques and procedures. To quote from Singer-Vine's appeal, "[A] technique is a technical method of accomplishing a desired aim and a procedure is a particular way of doing or going about accomplishment of something."[71] These broad definitions clearly encompass the technical methods of accomplishing the protection of the Commission's IT infrastructure and the way the Commission goes about accomplishing that goal.

29. And we reject Singer-Vine's suggestion that "it is entirely unclear what possibly could be expected to risk circumvention of the law."[72] In setting forth the risk of harm, an agency is not required to meet a "highly specific burden of showing how the law will be circumvented."[73] Rather, the agency need only "demonstrate logically how release of the requested information might create a risk of circumvention of the law."[74] The response staff sent to Singer-Vine detailed that "[t]he requested logs would publicly disclose information about how the FCC protects the security of ECFS and its other information assets."[75] Singer-Vine does not explain why that explanation is deficient under applicable case law. Further, as we discuss above, release of the server logs could allow malicious actors to discover vulnerabilities in the system and exploit those vulnerabilities to jeopardize the Commission's network security and evade detection. We find these reasons to be sufficient to withhold the server logs under Exemption 7(E).

30. Our decision to withhold the server logs under Exemption 7(E) is further supported by the recent district court opinion in *Prechtel v. Federal Communications Commission*. The plaintiff in *Prechtel* similarly sought certain ECFS server logs related to Docket No. 17-108.[76] Commission staff withheld the server logs under Exemption 7(E), citing a risk to the Commission's IT infrastructure.[77] The court affirmed this withholding, concluding that the Commission properly withheld the server logs under Exemption 7(E).[78] Given that the federal district court in D.C. has approved withholding of a functionally identical set of records, we conclude that staff properly withheld the server logs in response to Confessore and Singer-Vine's requests.

C. Segregability

31. The FOIA requires agencies to "take reasonable steps necessary to segregate and release nonexempt information."[79] As noted by staff in its response, the requested server logs consist of hundreds of millions of lines of technical information documenting the servers' activities. Those voluminous records are riddled with personal and security information in a way that makes it infeasible to segregate

[70] 2018-204 Appeal at 5.

[71] *Id.* at 5 (internal quotations and citations omitted).

[72] *Id.* at 5-6 (contending that "all the Agency has done is 'incant' those 'familiar' phrases that FOIA requesters are so used to seeing").

[73] *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1193 (D.C. Cir. 2009).

[74] *Id.* at 1194.

[75] 2018-204 Response at 1.

[76] *Prechtel* at *3.

[77] *Id.* at *10.

[78] *Id.* at *10.

[79] 5 U.S.C. § 552(a)(8)(A)(ii)(II). *See also* 5 U.S.C. § 552(b) ("Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt.").

the exempt from the non-exempt information.[80] Both Confessore and Singer-Vine challenge staff findings regarding the segregability of the logs.[81]

32. We affirm the staff conclusion that non-exempt information in the server logs cannot reasonably be segregated and provided to the requester. The task of removing IP addresses and sensitive security information from the logs would be an unreasonably burdensome undertaking. Redaction of exempt information is not a task that can be readily automated using the Commission's existing technology.[82] The effort would require either line-by-line review of hundreds of millions of lines of computer data or would require the Commission to invest considerable IT resources in programming new software to make the necessary redactions.[83] Neither of these are within the scope of the "reasonable steps" contemplated in the FOIA.[84]

D. Confessore Request Modification

33. After filing his appeal, Confessore offered to modify his request in the hopes of addressing the privacy and security concerns raised by staff. In particular, Confessore suggested the Commission could produce two separate logs, one showing the IP addresses from which comments originated, and a second showing certain computer information of those systems.[85] The two sets of logs would be linked by a unique identifier the Commission would assign to any given entry.

34. We deny this modified version of the request. Although agencies are required to conduct simple database searches under the FOIA,[86] the FOIA does not require agencies to create new records to satisfy requests.[87] Processing the request as modified by Confessore would go well beyond a straightforward database query; it would require the Commission to create records that do not already exist. In order to fulfill the request, the FCC would have to devote significant resources to developing and executing a new computer program that the agency does not currently possess. Commission technical specialists would have to write a computer program capable of analyzing each element of the data rows

[80] 2017-764 Supplemental Response Letter at 3-4.

[81] 2018-204 Appeal at 6; 2017-764 Supplemental Appeal at 5.

[82] Confessore argues that by limiting the scope of his FOIA request to the X-Forward-For header, date/time stamp of each request, IP address of the client making the request, and browser USERAGENT, he should effectively eliminate any security concerns the Commission has regarding release of the server logs. 2017-764 Supplemental Appeal at 2. However, as noted above, we conclude that IP addresses themselves are protected information. To the extent certain portions of information that Confessore requests, such as date/time stamps, do not themselves fall under a FOIA exemption, we conclude that they are inextricably intertwined with other exempt information contained in the logs.

[83] Singer-Vine's more limited request for twenty specific comments would not eliminate the need for this line-by-line review or software development, as the server logs are not kept in a manner to allow individual comments to be readily extracted.

[84] *See Milton v. Dep't of Justice*, 842 F. Supp. 2d 257, 260 (D.D.C. 2012) ("Records [are] not reasonably segregable where the agency attest[s] that it lack[s] the technical capability to edit the records in order to disclose non-exempt portions."). *See also Prechtel v. FCC* at *11. In *Prechtel*, the plaintiff argued that the Commission could acquire or develop software that would allow it to provide the plaintiff with the requested records. However, the court concluded that "[t]he Commission need not acquire new technological capacity in order to comply with disclosure requests and the FOIA does not require it to craft complicated algorithms to meet [plaintiff's] request." *Id.* at *11 (internal citations and quotations omitted).

[85] May 7 Letter; August 31 Letter.

[86] *Nat'l Sec. Counselors v. CIA*, 898 F. Supp. 233 (D.D.C. 2012).

[87] *See Students Against Genocide v. Dep't of State*, 257 F.3d 828 (D.C. Cir. 2001) (citing *Yeager v. DEA*, 678 F.2d 315, 321 (D.C. Cir. 1982)); *Center for Public Integrity v. FCC*, 505 F. Supp. 2d 106, 114 (D.D.C. 2007) (finding that the court could not require the FCC to redact documents in the manner proposed by the requester because the proposal required the creation of new records).

contained in the responsive server logs, and of modifying or extracting certain sensitive elements from these logs. In order to create the actual document requested, the Commission would then need to devote significant computing resources to applying this program to the millions of rows of responsive server log entries. This kind of extensive data analysis far exceeds the requirements of FOIA.[88]

IV. ORDERING CLAUSES

35. IT IS ORDERED that, pursuant to section 5(c)(5) of the Communications Act of 1934, as amended, 47 U.S.C. § 155(c)(5), and section 1.115(g) of the Commission's rules, 47 CFR § 1.115(g), the application for review filed by Nicholas Confessore and the application for review filed by Jeremy Singer-Vine ARE DENIED. Confessore and Singer-Vine may seek judicial review of this action pursuant to 5 U.S.C. § 552(a)(4)(B).[89]

36. The officials responsible for this action are: Chairman Pai and Commissioners O'Rielly, Carr, and Rosenworcel.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[88] *See supra* n.84.

[89] We note that as part of the Open Government Act of 2007, the Office of Government Information Services (OGIS) was created to offer mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect Confessore's or Singer-Vine's right to pursue litigation. Confessore and Singer-Vine may contact OGIS in any of the following ways:

Office of Government Information Services
National Archives and Records Administration
Room 2510
8601 Adelphi Road
College Park, MD 20740-6001
E-mail: ogis@nara.gov
Telephone: 301-837-1996
Facsimile: 301-837-0348
Toll-free: 1-877-684-6448.

STATEMENT OF
CHAIRMAN AJIT PAI

Re: ***Nicholas Confessore On Request for Inspection of Records*, FOIA Control No. 2017-764,**
***Jeremy Singer-Vine On Request for Inspection of Records*, FOIA Control No. 2018-204,**
Memorandum Opinion and Order

For many years as a Commissioner, I called on the FCC's leadership to publish FCC meeting items before the FCC held a vote.[1] I argued that this was basic good government—that an agency that regulates one-sixth of the economy should be transparent and "show its work" in advance to the American people. My dissenting colleague said—nothing.

In 2014, the FCC withheld documents created by a private law firm on behalf of a private client from disclosure under the Freedom of Information Act (FOIA) exemption for "intra-agency" documents (that is, solely within this agency).[2] I dissented, arguing that it was absurd to suggest that a document generated outside this agency by an outside law firm doing work for an outside client could be considered an "intra-agency" document. My dissenting colleague said—nothing.

In 2015, before the FCC rammed through utility-style Internet regulation under White House pressure, I called on the agency to publish the draft order so that the American people could see all 300-plus pages of it before the decision was actually made.[3] My dissenting colleague said—nothing.

In 2016, the FCC considered major reforms to the Universal Service Fund's program for small, rural carriers. Commissioner O'Rielly, who played a leading role in drafting these reforms, and I requested the reforms be published ahead of a vote, and the head of a major rural broadband association explicitly said "It is absolutely essential to see the written words on the page and review the specific terms of the order to understand the actual effectiveness of the reforms." Our request was denied. My dissenting colleague said—nothing.

In the nearly half-decade preceding this Administration, there arose many, many chances to join what should have been a bipartisan effort to promote openness and transparency at the FCC. And yet, my dissenting colleague said—nothing.[4]

---

[1] *See*, *e.g.*, Hearing before House Energy and Commerce Committee, Subcommittee on Communications and Technology, Witness Statement of Commissioner Pai at 3 (Mar. 22, 2016), *available at* https://docs.house.gov/meetings/IF/IF16/20160322/104714/HHRG-114-IF16-Wstate-PaiA-20160322.pdf ("Take this simple proposition: The public should be able to see what we're voting on before we vote on it. That's how Congress works, as you know. Anyone can look up any pending bill right now by going to congress.gov. And that's how many state commissions work too. But not the FCC.").

[2] *Greenberg Traurig, LLP, on Request for Inspection of Records*, FOIA Control No. 2013-025, Memorandum Opinion and Order, 29 FCC Rcd 12045 (2014).

[3] *See*, *e.g.*, https://twitter.com/ajitpaifcc/status/563724099906568193.

[4] *See*, *e.g.*, Hearing before House Energy and Commerce Committee, Subcommittee on Communications and Technology, Preliminary Transcript at 91-92 (Mar. 22, 2016), *available at* https://docs.house.gov/meetings/IF/IF16/20160322/104714/HHRG-114-IF16-Transcript-20160322.pdf:

> "Mr. Pai. Whoever is leading the agency, Republican or Democrat, I would hope that they would embrace the same spirit of transparency that the Congress has, in terms of making things public before they are voted upon.
>
> Mr. Lance. Commissioner Rosenworcel, your comments on the discussion I have had with your colleagues?
>
> Ms. Rosenworcel. Well, thank you. I have not found that our existing policies get in the way of me having substantive conversations with stakeholders of every stripe.
>
> . . .

But that was then. Today, we see newfound advocacy of transparency arising in this FOIA decision. In making this decision, the FCC relies on clear judicial precedent and careful analysis of the facts to uphold the career staff's determination that disclosure of certain server logs is inappropriate under FOIA Exemptions 6 and 7(E). Among many other things, the agency painstakingly explains U.S. Supreme Court precedent discussing Exemption 6 and analyzes why that exemption applies here. The agency also relies on a very recent decision by an Obama appointee to the U.S. District Court for the District of Columbia involving *these very server logs*, holding that the agency's justification for applying the 7(E) exemption "more than suffices" for purposes of FOIA.[5]

My dissenting colleague says—a lot. But nothing about the U.S. Supreme Court precedent. Nothing about the on-point district court decision. Nothing about why our career information technology staff's determination that releasing these server logs could undermine our agency's efforts to defend against cyberattacks is wrong. Indeed, nothing whatsoever about any of the actual analysis the FCC or its career staff have proffered.

Instead, one finds the now-standard overheated rhetoric about "net neutrality" (omitting, as usual, the fact that the half-million comments submitted from Russian e-mail addresses and the nearly eight million comments filed by e-mail addresses from e-mail domains associated with FakeMailGenerator.com supported her position on the issue!).

What has changed between then and now? Literally nothing, other than the political affiliation of the FCC's leadership (and a lot more transparency now than the agency ever had then). What is required in this matter, as in any other, is sober analysis of the facts and the law—not partisan gamesmanship. Fortunately, the Commission majority embraces that ethos in this item.

(Continued from previous page)

> Mr. Lance. In your opinion, do you and I have a right to go back and forth in the document that Commissioner Pai has at his desk?
>
> Ms. Rosenworcel. I believe we have the right to go back and forth and discuss any matter that is before the agency.
>
> Mr. Lance. I don't know what is contained in that document. Are you able to release to me what is contained in that document?
>
> Ms. Rosenworcel. I don't believe we are.
>
> Mr. Lance. And why is that, Commissioner?
>
> Ms. Rosenworcel. I believe that is under our Commission's rules right now.
>
> Mr. Lance. . . . Do you agree with the rules?
>
> Ms. Rosenworcel. I think that we can do more so that our discussions are transparent but I also think it is essential that we preserve the right to have deliberations among the five of us and actually review the text and discuss the text among all of us. So, I think we should strive to be more transparent but I think we have to preserve some space for honest deliberation."

[5] *Prechtel v. FCC*, Case No. 17-cv-01835 (CRC), slip op. at 22 (Sept. 13, 2018).

STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL,
DISSENTING

Re: ***Nicholas Confessore On Request for Inspection of Records*, FOIA Control No. 2017-764,**
***Jeremy Singer-Vine On Request for Inspection of Records*, FOIA Control No. 2018-204,**
Memorandum Opinion and Order

What is the Federal Communications Commission hiding?

Since 1946, the Administrative Procedure Act has charged agencies making major policy decisions with the responsibility to open their process to the public. They are required to give "interested persons" an opportunity to voice their opinions, and only after considering these public comments may agencies proceed with proposed policies and adopt new rules.

This system may have served Washington policymaking well for decades, but it is showing its age. In proceedings at this agency and others, the public is increasingly shut out of decision-making by the fraud that is flooding public channels for comment.

You see this every clearly in the FCC's net neutrality proceeding. Last year, when the agency made the misguided decision to roll back its net neutrality rules, it did so based on a public record littered with problems. While millions of Americans sought to inform the FCC process by filing comments and sharing their deeply-held opinions about internet openness, millions of other filings in the net neutrality docket appear to be the product of fraud. As many as nine and a half million people had their identities stolen and used to file fake comments, which is a crime under both federal and state laws. Nearly eight million comments were filed from e-mail domains associated with FakeMailGenerator.com. On top of this, roughly half a million comments were filed from Russian e-mail addresses.

Something here is rotten—and it's time for the FCC to come clean.

Regrettably, this agency will not do this on its own. So it falls to those who seek to investigate from outside its walls. To this end, two journalists—from the New York Times and BuzzFeed News—sought to obtain records related to the FCC's net neutrality record, pursuant to the Freedom of Information Act. With this information, they will have the material they need to review where this fraud in our public record came from, assess who could have orchestrated it, and identify who could have paid for it to occur.

But instead of providing news organizations with the information requested, in this decision the FCC decides to hide behind Freedom of Information Act exemptions and thwart investigative journalism. In doing so, the agency asserts an overbroad claim about the security of its *public* commenting system that sounds no more credible than its earlier and disproven claim that the system was the subject of distributed denial of service attack. It appears this agency is trying to prevent anyone from looking too closely at the mess it made of net neutrality. It is hiding what it knows about the fraud in our record and it is preventing an honest account of its many problems from seeing the light of day. I dissent.