Filed
United States Foreign
Intelligence Surveillance Court

JUN 2 5 2020

LeeAnn Flynn Hall, Clerk of Court

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE CARTER W. PAGE, A U.S. PERSON	**Docket Nos:** 16-1182, 17-52, 17-375, 17-679

OPINION AND ORDER REGARDING USE AND DISCLOSURE OF INFORMATION

On four occasions in 2016 and 2017, upon application by the government in the above-captioned dockets, the Foreign Intelligence Surveillance Court approved electronic surveillance and physical search targeting Carter W. Page pursuant to the Foreign Intelligence Surveillance Act, *codified as amended at* 50 U.S.C. §§ 1801-1885c. The government has acknowledged that at least some of its collection under color of those FISC orders was unlawful. It nevertheless now contends that it must temporarily retain, and potentially use and disclose, the information collected, largely in the context of ongoing or anticipated litigation. The Court hereby sets parameters for such use or disclosure.

I. Background

Prior orders of this Court have discussed material errors and omissions in the applications in the above-captioned dockets, which errors pertained to whether there was probable cause to believe that Page was an agent of a foreign power. See Corrected Op. and Order, Misc. No. 19-02 (FISA Ct. Mar. 5, 2020); Order, Misc. No. 19-02 (FISA Ct. Dec. 17, 2019). Those errors and omissions were largely uncovered by the Office of the Inspector General, U.S. Department of

Justice. See OIG, DOJ, Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation (Dec. 2019 (revised)) ("OIG Report").

On December 9, 2019, the government advised the Court of its assessment that, for the applications in Docket Numbers 17-375 and 17-679, "if not earlier, there was insufficient predication to establish probable cause to believe that Page was acting as an agent of a foreign power." Additional Rule 13(a) Letter Regarding Applications Submitted to the Ct. Targeting Carter W. Page in Docket Nos. 2016-1182, 2017-0052, 2017-0375, and 2017-0679, at 19 (Dec. 9, 2019). The government further reported that the FBI would "sequester all collection the FBI acquired pursuant to the Court's authorizations in the above-listed four docket numbers . . . pending further review" of the OIG Report and "the outcome of related investigations and any litigation." Id. at 19-20 (emphasis added). Information acquired under color of the above-captioned dockets, in both minimized and un-minimized (i.e., raw) form, will be referred to as "Page FISA information."

On January 7, 2020, the Court ordered the government to explain how it is restricting access to the Page FISA information and why its retention and any contemplated use or disclosure are necessary and lawful. See Order Regarding Handling and Disposition of Information at 2, Nos. 16-1182, 17-52, 17-375, 17-679 (FISA Ct. Jan. 7, 2020), *declassified version available at* https://fisc.uscourts.gov/public-filings/order-regarding-handling-and-disposition-information. The government responded on February 5, February 28, and April 17, 2020. See Resp. to the Ct.'s Order Dated Jan. 7, 2020, Nos. 16-1182, 17-52, 17-375, 17-679 (Feb. 5, 2020); Supplemental Resp. to the Ct.'s Order Dated Jan. 7, 2020, Nos. 16-1182, 17-52, 17-375, 17-679 (Feb. 28, 2020); Second Supplemental Resp. to the Ct.'s Order Dated Jan. 7, 2020, Nos. 16-1182, 17-52, 17-375, 17-679 (Apr. 17, 2020).

II. Analysis

After examining the relevant provisions of FISA, the Court will evaluate the grounds put forward by the government for retaining, using, and disclosing Page FISA information.

A. The Relevant Statutory Provisions

FISA restricts the use and disclosure of information acquired by unauthorized electronic surveillance or physical search that was conducted under color of a FISA authorization. See 50 U.S.C. §§ 1809(a)(2), 1827(a)(2). It also has minimization requirements, which regulate the retention and dissemination of FISA-acquired information generally.

1. Sections 1809(a)(2) and 1827(a)(2)

It is a criminal offense to "intentionally . . . (1) engage[ ] in electronic surveillance under color of law except as authorized by" identified statutory provisions, or "(2) disclose[ ] or use[ ] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized" by FISA or another "express statutory authorization." § 1809(a). It is similarly an offense to intentionally conduct a physical search under color of law within the United States to obtain foreign-intelligence information, "except as authorized by statute," or intentionally disclose or use information obtained by such a search, "knowing or having reason to know that the information was obtained through physical search not authorized by statute, for the purpose of obtaining intelligence information." § 1827(a).

The government acknowledges that there were material omissions, and the Court has found violations of the government's duty of candor, in all four applications. See Resp. to the Ct.'s Corrected Op. and Order Dated Mar. 5, 2020, and Update to the Gov't's Jan. 10, 2020, Resp. at 20-21, Misc. No. 19-02 (Apr. 3, 2020); Order at 2-3 & nn.7-8, Misc. No. 19-02 (FISA

Ct. Dec. 17, 2019). As noted above, the government admits that at least the third and fourth Page applications lacked adequate factual support. See Dec. 9, 2019, Letter at 2, 19. It further admits that "the restrictions on use or disclosure in Sections 1809 and 1827 apply at least" to information acquired under color of the third and fourth dockets, without addressing whether they apply to information acquired under color of the first two dockets. See Feb. 5, 2020, Resp. at 28. In fact, in response to the Court's directive to explain why retaining the Page FISA information "in the manner intended by the government, and any contemplated use or disclosure of it," comport with §§ 1809(a)(2) and 1827(a)(2), Jan. 7, 2020, Order at 2, the government declined to argue, even alternatively, that those provisions do not apply (or apply differently) to information obtained under the first two dockets. See Feb. 5, 2020, Resp. at 28-29. Under the circumstances, the Court will assume that §§ 1809(a)(2) and 1827(a)(2) apply to information acquired under color of the first and second dockets just as, per the government's admission, they apply to information acquired under color of the third and fourth.

Proceeding from that premise, the plain meaning of those statutory provisions prohibits intentional use or disclosure of the Page FISA information by anyone who knows or has reason to know it was acquired by unauthorized electronic surveillance or physical search. The FISC has, however, recognized an exception to the unqualified language of § 1809(a)(2) for "actions that are necessary to mitigate or prevent the very harms at which [that section] is addressed." See Op. and Order Regarding Fruits of Unauthorized Elec. Surveillance, Nos. 06-1482, et al., at 8 (FISA Ct. Dec. 10, 2010) ("December 10, 2010, Opinion and Order") (emphasis in original). (That prior case did not involve physical search and therefore did not implicate § 1827(a)(2).) Specifically, some uses or disclosures may be "necessary to avoid similar instances of over-collection . . . or to remedy a prior over-collection." Id. at 7. The Court recognized that

exception because, "in limited circumstances, prohibiting use or disclosure of the results of unauthorized electronic surveillance would be so absurd or glaringly unjust . . . as to [call into] question whether Congress actually intended what the plain language of Section 1809(a)(2) so clearly imports." Op. and Order Requiring Destruction of Information Obtained by Unauthorized Elec. Surveillance at 5, Nos. 06-1482, et al. (FISA Ct. May 13, 2011) (quoting United States v. Rodgers, 466 U.S. 475, 484 (1984)) ("May 13, 2011, Opinion").

2. Minimization Provisions

The government must also handle information obtained by FISA electronic surveillance and physical search in accordance with FISC-approved minimization procedures. For electronic surveillance, there must be "specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination" of private information about unconsenting U.S. persons "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1). Notwithstanding that requirement, the procedures should "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." § 1801(h)(3). Substantively identical minimization requirements apply to FISA physical searches. See 50 U.S.C. § 1821(4)(A), (C). In order to approve an electronic surveillance or physical search, the Court must find that the procedures satisfy these requirements and direct that they be followed. See 50 U.S.C. §§ 1805(a)(3), (c)(2)(A); 1824(a)(3), (c)(2)(A).

In this case, the applicable minimization procedures have a "litigation-hold" provision under which the FBI "may temporarily retain," subject to restricted-access requirements,

"specific FISA-acquired information that would otherwise have to be destroyed pursuant to these minimization procedures, [redacted] [redacted] [redacted]." Standard Minimization Procedures for FBI Elec. Surveillance and Physical Search Conducted Under the FISA § III.I.4 at 41 (May 17, 2016) ("FBI SMPs") (emphasis added). But that provision does not apply to the Page FISA information because that information does not otherwise have to destroyed pursuant to the FBI SMPs. The FBI SMPs, in other words, do not contain a provision requiring the FBI to destroy the results of unauthorized surveillance or search. A separate provision, moreover, confirms that Section III.I.4 does not authorize retention of the Page FISA information: "Nothing in these Procedures permits the retention of information obtained through unauthorized electronic surveillance or physical search." FBI SMPs § III.F at 31 n.10 (emphasis added).

B. The Government's Grounds for Retaining, and Potentially Using and Disclosing, the Page FISA Information

Having now set the statutory backdrop, the Court may examine the government's discrete positions here. The government contemplates retention, use, and disclosure of some or all of the Page FISA information in several contexts, specifically: (1) ongoing litigation with third-party plaintiffs pursuant to the Freedom of Information Act, see Apr. 17, 2020, Resp. at 9-10; Feb. 28, 2020, Resp. at 10-11; Feb. 5, 2020 Resp. at 27; (2) ongoing and anticipated civil litigation with Page, see Apr. 17, 2020, Resp. at 7-8; Feb. 28, 2020, Resp. at 8-9; Feb. 5, 2020, Resp. at 26-27; (3) FBI review of the conduct of its personnel in the Page investigation, see Apr. 17, 2020, Resp. at 7; (4) DOJ OIG's monitoring of the implementation of the recommendations in the OIG Report and auditing of the FBI's compliance with its accuracy procedures (also called "Woods"

procedures), see Feb. 5, 2020, Resp. at 20; and (5) review of, [redacted] the conduct of government personnel in the Page investigation and the broader "Crossfire Hurricane" investigation of Russian interference in the 2016 Presidential election. See id. at 25-26.

Before drilling down on these specific contexts, some general observations may prove helpful. To begin, retention must be distinguished from use and disclosure. Regarding retention, the government asserts that "all of the information from the above four dockets needs to be preserved" in order for it "to comply with . . . discovery obligations that may arise in the current civil litigation, as well as any discovery obligations that may arise in the future vis-`a-vis other possible litigation." Feb. 5, 2020, Resp. at 36; Feb. 28, 2020, Resp. at 11. Much, if not all, of such information is indeed subject to pending FOIA litigation brought by Page. See infra p. 12. Importantly, neither FISA nor the applicable minimization procedures explicitly require the government to destroy the Page FISA information. See supra pp. 3, 6. It is true that, even absent such a requirement, the FISC has nonetheless ordered destruction of information obtained through unauthorized physical search when there was no reason to anticipate circumstances in which use or disclosure would be permitted. See Order Requiring Destruction of Information Obtained By Unauthorized Physical Searches at 3-4, Nos. 18-45, 19-403 (FISA Ct. Oct. 21, 2019). Those circumstances are distinguishable because, as discussed below, some permissible forms of use and disclosure of Page FISA information are reasonably anticipated here.

Moving beyond retention, not all of the government's arguments regarding use and disclosure are persuasive. First, it contends that "strict access controls [will] ensure" that the Page FISA information "may not be used for analysis or further investigation." Feb. 5, 2020, Resp. at 36; Feb. 28, 2020, Resp. at 11; Apr. 17, 2020, Resp. at 10. But a FISC judge previously

rejected the interpretation that § 1809(a)(2) only prohibits use or disclosure for investigative or analytical purposes. See Dec. 10, 2010, Op. and Order at 6-7. And notwithstanding its disavowal of analytical or investigative use, the government contemplates use and disclosure of the Page FISA information not only in civil litigation, but also in the course of performance and disciplinary reviews of the conduct of FBI personnel, as well as potential criminal prosecutions.

The government also argues that "Congress did not intend FISA or . . . [FISA] minimization procedures . . . to abrogate the rights afforded to defendants in criminal proceedings" and submits without explanation "that the same reasoning would apply in civil proceedings." Feb. 5, 2020, Resp. at 34-35. The only authority cited for the initial premise is a discussion in legislative history of provisions that, as modified, were enacted and codified at 50 U.S.C. § 1806: "[N]othing in these subsections [of what became § 1806] abrogates the rights afforded a criminal defendant under Brady v. Maryland, and the Jencks Act." H.R. Rep. No. 95-1283, pt. I, at 89 (1978) (emphasis added, footnotes omitted); see also S. Rep. No. 95-604, pt. 1, at 55-56 (1978)) (same). By its terms, that statement says nothing about the intended effect of §§ 1809(a)(2) and 1827(a)(2). (The Jencks Act, 18 U.S.C. § 3500, requires production of a prosecution witness's prior statements. Brady v. Maryland, 373 U.S. 83 (1963), requires production of material evidence favorable to a criminal defendant upon request.)

Section 1806 establishes procedures, moreover, for a court to determine the legality of an electronic surveillance before information thereby obtained is used against an aggrieved person in a legal proceeding. In contrast, §§ 1809(a)(2) and 1827(a)(2) specifically address the circumstances of this case, where we already know that information was obtained through unlawful surveillance and search, but the government contemplates using and disclosing it anyway.

More fundamentally, any tension between the prohibitions of §§ 1809(a)(2) and 1827(a)(2) and the rights of a potential criminal defendant can be eliminated by the government's forgoing the prosecution in which use or disclosure of the results of unauthorized surveillance or search would be necessary. Potentially letting the guilty escape prosecution is a heavy burden for the government, and the public, to bear. But "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty." Nardone v. United States, 302 U.S. 379, 383 (1937) (holding that statutory prohibition on intercepting a communication and divulging or publishing its contents barred federal agents from testifying at a criminal trial about what they overheard on a wiretap). Congress may also have sought to avoid the further intrusion into the privacy of persons subjected to unlawful surveillance that would result from prosecutorial use of surveillance information. The unqualified language of §§ 1809(a)(2) and 1827(a)(2) evidences that Congress intended for the government to be deprived of such prosecutorial uses, at least in some cases.

Because the government's broad-brush arguments on use and disclosure are unpersuasive, the Court will separately examine each context in which the government contemplates use or disclosure of the Page FISA information.

1. Third-Party FOIA Litigation

The government has identified two third-party FOIA cases that implicate records that contain some of the Page FISA information in apparently minimized form:

(1) Judicial Watch, Inc. v. DOJ, No. 18-1854 (D.D.C.), in which "plaintiffs seek, *inter alia*, all records from [the Office of the Deputy Attorney General (ODAG)] relating to Fusion GPS, Nellie Ohr and/or British national Christopher Steele." Feb. 28, 2020, Resp. at 10. ODAG possessed "copies of the Page FISA applications and related memos that

contain FISA-acquired information," as well as notes and classified emails "that may be responsive to this Judicial Watch FOIA request" and might contain FISA-acquired information. Id. at 10-11.

(2) James Madison Project v. DOJ, No. 17-597 (D.D.C), in which the plaintiff challenges some of the redactions in publicly available versions of the Page FISA applications and orders. See Feb. 5, 2020, Resp. at 27.

Page is not a party to either case. The government has also mentioned, without identifying, ongoing FOIA litigation regarding records of the former Special Counsel's Office (SCO), which apparently also involves a record containing Page FISA information in minimized form. See id. at 8-10.

Litigation with third-party FOIA requesters does not fit into the previously recognized exception to §§ 1809(a)(2) and 1827(a)(2) for preventing or remedying unauthorized electronic surveillance or physical search. It is clear, however, that FOIA applies to records that an agency has created or obtained and that are within its control when a FOIA request is made, see Grand Cent. P'ship, Inc. v. Cuomo, 166 F.3d 473, 479 (2d Cir. 1999), and that a requester may seek district court review of whether records have been improperly withheld. See 5 U.S.C. § 552(a)(4)(B). FOIA does not require disclosure of "matters that are . . . specifically exempted from disclosure by statute" if the statute "requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue . . . or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3)(A).

Statutes "enacted after the date of enactment of the Open FOIA Act of 2009" must also "specifically cite[ ]" § 552(b)(3) to provide a basis for invoking this exemption from disclosure. See § 552(b)(3)(B). But that citation requirement does not apply to §§ 1809(a)(2) and 1827(a)(2). The Open FOIA Act was enacted on October 28, 2009. See Dep't of Homeland Security Appropriations Act, 2010, Pub. L. No. 111-83, § 564, 123 Stat. 2142, 2184 (2009).

Section 1809(a)(2) was originally enacted in 1978, see FISA, Pub. L. No,. 95-511, § 109(a)(2), 92 Stat. 1783, 1796 (1978), and since October 28, 2009, has only been amended to correct punctuation. See Intelligence Authorization Act for Fiscal Year 2010, Pub. L. No. 111-259, § 801(3), 124 Stat. 2654, 2746 (2010). Section 1827(a)(2) was enacted in 1994 and has not been amended. See Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807(a)(3), 108 Stat. 3423, 3452 (1994).

Because FOIA exempts such information from disclosure, it does not necessarily conflict with §§ 1809(a)(2) and 1827(a)(2) regarding whether the Page FISA information should be disclosed to the third-party plaintiffs. (Other FOIA exemptions may also apply. See, e.g., § 552(b)(6) (protecting against unwarranted invasion of personal privacy)). But, as a practical matter, that FOIA litigation could not proceed if §§ 1809(a)(2) and 1827(a)(2) were further understood, for example, to bar FBI and other DOJ personnel working on that litigation from using or disclosing such information among themselves, insofar as it appears in documents responsive to the pertinent FOIA requests.

When different statutes apply to the same circumstances, a court "is not at liberty to pick and choose among congressional enactments and must instead strive to give effect to both." Epic Sys. Corp. v. Lewis, 138 S. Ct. 1612, 1624 (2018) (quoting Morton v. Mancari, 417 U.S. 535, 551 (1974)). Accordingly, the Court construes the applicable statutes to permit use or disclosure of Page FISA information insofar as necessary for the good-faith conduct of the above-described third-party FOIA litigation. The Court anticipates that any Page FISA information subject to use or disclosure in the context of such litigation, including within FBI and DOJ, will be limited to what is contained in the records responsive to the third-party FOIA

requests. The Court also expects that the government will take into account the strictures of §§ 1809(a)(2) and 1827(a)(2) in assessing what should be disclosed to the plaintiffs.

2. Page's Civil Litigation

The government advises that, on October 12, 2019, Page himself filed a complaint against DOJ alleging FOIA and Privacy Act violations, including that he was improperly denied access to his own records. See Feb. 5, 2020, Resp. at 26 (citing Page v. U.S. Dep't of Justice, No. 19-3149 (D.D.C.)). The Complaint alleges that on May 21, 2017, Page "submitted requests to the DOJ, FBI and NSA under the Privacy and Freedom of Information Acts for copies of all information . . . about himself" and requests that the district court order disclosure to Page of "the previously requested records in their entireties," apparently in order to identify and "expunge all records or information maintained by the DOJ that [are] inaccurate and/or derogatory" to him. See Complaint at 7, 9. The government further reports that Page's attorneys have advised DOJ of more claims that he may bring against the government, "including violations of the Patriot Act, FISA, the Privacy Act, and the Federal Tort Claims Act." See Apr. 17, 2020, Resp. at 8; Feb. 28, 2020, Resp. at 9.

The analysis set out above for the third-party FOIA litigation points to the same conclusion for Page v. U.S. Dep't of Justice: it is permissible for the government to use or disclose the Page FISA information insofar as necessary to its good-faith conduct of that litigation. The litigation with Page nonetheless presents circumstances notably different from the third-party FOIA litigation. First, the litigation with Page involves much more Page FISA information, including much if not all of the raw results of electronic surveillance and physical search targeting him. Second, there may be reasonable arguments that §§ 1809(a)(2) and 1827(a)(2) should not be interpreted to prohibit disclosure of information in response to a

request from the target of the unauthorized surveillance or search by which the information was obtained. That issue should be resolved, if necessary, in the district court litigation.

Finally, although the Court cannot know the exact nature of claims that Page has not yet brought, it is foreseeable that they may seek redress for alleged injury from the unauthorized surveillance and search. The FISC has previously found that "Congress may be presumed not to have prohibited actions that are necessary to mitigate or prevent the very harms at which Section 1809(a)(2) is addressed," see Dec. 10, 2010, Op. at 8 (emphasis in original, internal quotation marks omitted), in order to avoid a result "so absurd or glaringly unjust" that it calls into question "whether Congress actually intended what the plain language" of § 1809(a)(2) seemingly requires. See May 13, 2011, Op. at 5 (quoting Rodgers, 466 U.S. at 484). It would be similarly anomalous to interpret §§ 1809(a)(2) and 1827(a)(2) as impeding a target of unlawful surveillance or search from pursuing civil remedies – e.g., by preventing discovery of surveillance information necessary to prove the existence or scope of the surveillance. FISA itself, moreover, affords a cause of action to an aggrieved person who has "been subjected to an [unauthorized] electronic surveillance or about whom information obtained by electronic surveillance of such person[s] has been disclosed or used in violation of" § 1809. See 50 U.S.C. § 1810. (A comparable civil-liability provision regarding unauthorized physical searches appears at § 1828.) Interpreting FISA's criminal prohibitions to hinder pursuit of its complementary civil remedies would violate the principle that "[s]tatutes should be interpreted as a symmetrical and coherent regulatory scheme." Mellouli v. Lynch, 575 U.S. 798, 135 S. Ct. 1980, 1989 (2015) (quoting FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000)). The Court consequently concludes that §§ 1809(a)(2) and 1827(a)(2) do not prohibit use or disclosure insofar as necessary for the good-faith conduct of litigation of any future claims

brought by Page seeking redress for unlawful surveillance and search or disclosure of the results of such surveillance and search.

3. Review of FBI Personnel's Conduct

The FBI's Inspection Division (INSD) has access to the Page investigative file in a storage system called Sentinel. See Apr. 17, 2020, Resp. at 17. The government submits that INSD "needs access to the case file as part of its review of the conduct of personnel involved in the Page investigation." Id. That file contains, in minimized form, some information acquired under color of the above-captioned dockets. INSD personnel have been instructed not to further use or disclose such information "without discussing the matter with FBI's [Office of General Counsel (OGC)], whose personnel will notify NSD." Id. Previously, INSD received hard copies of the Page FISA renewal applications and associated Woods files, which also contain minimized FISA information. See Feb. 5, 2020, Resp. at 7-8; Feb. 28, 2020, Resp. at 7 n.8. It also possesses in electronic form "minimized, and potentially unminimized, information obtained pursuant to the authorities granted in the above dockets," which the government has not further described. See Feb. 5, 2020, Resp. at 7.

The Court understands INSD's review to include a performance assessment of FBI personnel's conduct of the Page investigation, as well as potentially an assessment of whether disciplinary actions are appropriate for particular personnel. See Corrected Op. and Order at 14-15, Misc. No. 19-02 (FISA Ct. Mar. 5, 2020). The disciplinary assessment may also involve the FBI's Office of Professional Responsibility (OPR). Id. In the abstract, identifying deficient performance and holding personnel accountable for misconduct in the FISA process plausibly fall within the previously recognized exception to §§ 1809(a)(2) and 1827(a)(2) for use and disclosure to prevent unauthorized surveillance or search. But the Court has emphasized that the

exception applies only when use or disclosure of specific information is necessary for such a purpose. See May 13, 2011, Op. at 4-7. The FISC in that case sought to delineate the exception narrowly because it is "for Congress to resolve the pros and cons of whether a statute should sweep broadly or narrowly." Id. at 5 (quoting Rodgers, 466 U.S. at 484). The court was also mindful that it "should not attempt to restrict the unqualified language of a [criminal] statute to the particular evil that Congress was trying to remedy–even assuming that it is possible to identify that evil from something other than the text of the statute itself." Id. (quoting Brogan v. United States, 522 U.S. 398, 403 (1998)). In that case, the National Security Agency sought to use the results of a particular unauthorized surveillance for auditing or "other aspects of an enterprise-wide compliance program." Id. at 7. The FISC held that the exception did not apply because "the specific over-collected information at issue no longer ha[d] any distinctive utility for NSA's compliance efforts." Id. (emphasis added). Accordingly, it was "neither absurd, nor glaringly unjust, nor obviously at variance with the policy of FISA as whole" to hold the government to the plain meaning of § 1809(a)(2). Id.

Applying those standards to this case, the Court is satisfied that effective performance or disciplinary reviews of the relevant FBI personnel require access to records such as the Page case file and applications, including the relatively limited and presumably minimized FISA information therein. The same cannot be said of access to the entire body of Page FISA information retained in raw form, much of which presumably was not found to be relevant to the investigation. It is possible, however, that such reviews may legitimately require use or disclosure of specific raw information – e.g., if the contents of raw information accessed by a particular employee at a certain time are important to evaluating the employee's conduct. The Court therefore concludes that use or disclosure of raw information in the context of such

reviews is permissible only when a particular need has been demonstrated to use or disclose specific information.

4. Ongoing DOJ OIG Oversight

DOJ OIG is in possession of materials that contain "a limited amount" of Page FISA information: "1) each of the three renewal applications," including drafts; "2) the accuracy sub-file, or Woods File, for each renewal application; and 3) e-mail communications of FBI personnel who were assigned to the Crossfire Hurricane investigation and [DOJ National Security Division (NSD)] personnel who were involved with the Page applications." Feb. 5, 2020, Resp. at 18. OIG also received copies of documents from such NSD personnel and of emails and documents from others within NSD who received information about the Page investigation; "[i]t is possible that some of these documents and emails . . . may have included minimized summaries" of some of the Page FISA information. Id. at 15-16.

OIG finalized its report and concluded its investigation of the FBI's handling of the Page FISA applications on December 8, 2019. See Dec. 9, 2019, Letter at 20. Nonetheless, OIG is monitoring implementation of the recommendations in its report and responding to questions from members of Congress (which the government represents will not involve disclosure of any Page FISA information). See Feb. 5, 2020, Resp. at 20. OIG is also engaged in "an audit of the FBI's compliance with its Woods Procedures in FISA applications relating to U.S. persons." Id.

Most of the OIG's recommendations are systemic. See OIG Report at 414-17. The only one for which the Page FISA information could be relevant is Recommendation 9: that the "FBI should review the performance of all employees who had responsibility for the preparation, Woods review, or approval of the FISA applications [for Page], as well as the managers, supervisors, and senior officials in the chain of command of the Carter Page investigation." Id.

at 417. Some use or disclosure of Page FISA information may be permissible during such a review, see supra pp. 14-16, and the same reasoning extends to OIG's monitoring of its related recommendation. It is difficult to see how information about Page's private communications and activities could be relevant to assessing implementation of the other recommendations. And it is a stretch to think that information from unauthorized search and surveillance of one target will bear on evaluating the FBI's compliance with accuracy procedures in working on applications for unrelated targets. As a result, the Court finds that further use or disclosure of Page FISA information by OIG is permissible only insofar as necessary to its assessment of the implementation of Recommendation 9.

5. Ongoing Criminal Investigations and Potential Prosecutions

At the direction of the Attorney General, John H. Durham, the United States Attorney for the District of Connecticut, is leading "a review of intelligence activities relating to campaigns in the 2016 U.S. Presidential election and certain related matters." Feb. 5, 2020, Resp. at 24-25 (internal quotation marks omitted). That review "includes an investigation of the actions of government officials related to Carter Page generally and the decision to seek and continue monitoring him pursuant to FISA specifically." Id. at 25. It also encompasses a criminal investigation based on OIG's referral of actions taken by an FBI attorney in connection with the last Page application. The attorney altered the contents of a communication from another agency about Page's prior reporting relationship with the agency before forwarding it to the FBI agent who swore to the facts in the application. Id. at 25; OIG Report at 254-56.

Durham's team has received copies of the emails produced to OIG (see supra p. 16) and possesses "copies of FBI's Woods files for the Page FISA applications and other FBI documents that likely contain FISA-acquired information," as well as "handwritten notes and other

documents from FBI and SCO personnel" that may do so. See Feb. 5, 2020, Resp. at 21. Durham's team does "not have access to unminimized FISA-acquired information from the above dockets in FBI systems"; however, members of the team "who are FBI personnel have access to the records related to [the Page] case in FBI's Sentinel system." Id. (Sentinel includes the Page investigative files, which contain some Page FISA information in minimized form. See supra p. 14.) FBI team members also have access to copies of certain electronic communications of FBI personnel, which they can share with other team members. See Feb. 5, 2020, Resp. at 21-22. Those communications could include some Page FISA information. Id.

Beyond what has already been received, "U.S. Attorney Durham has requested that information relevant to [REDACTED] specific criminal referral [regarding the FBI attorney] . . . be preserved during the pendency [REDACTED]" Id. at 26. In the government's view, "FISA information acquired . . . [by] targeting Page . . . [and] retained in any form" is relevant [REDACTED] Id. [REDACTED] It also posits that "[i]t is possible that" Page FISA information "may be relevant to any ongoing investigation or resolution" of the criminal referral because it "may (I) constitute or relate to evidence of improper and/or criminal conduct committed by the FBI attorney [REDACTED] and/or (ii) constitute Jencks Act material, Brady material, or otherwise discoverable material relevant to a subject's defense, for example, on the issue of materiality." Id. at 25-26 (footnotes omitted, emphasis added). The government thus anticipates that such information may be used affirmatively to prove its case or be subject to obligations of disclosure to the defense.

In addition to prohibiting use or disclosure of the results of unauthorized electronic surveillance and physical search, §§ 1809 and 1827 make it a criminal offense under certain circumstances to intentionally engage in unauthorized electronic surveillance or physical search. See supra p. 3. Sections 1809 and 1827 would be self-defeating if they were interpreted to prohibit use or disclosure of such information, even when necessary to investigate and prosecute the very crimes they define. Beyond that, investigating and prosecuting other offenses that arise from misconduct by government personnel in the FISA process should deter future unauthorized surveillance and search, which may permit related uses or disclosures if needed for the previously recognized exception to the prohibition. See supra pp. 4-5, 14-15.

The government has not shown, however, that all of the Page FISA information is necessary to investigate or prosecute such violations. Certain materials, such as the Page investigative file, appear relevant to evaluating the conduct of FBI personnel during that investigation, but, taken as a whole, the larger body of un-minimized search and surveillance results does not. See supra p. 15. For purposes of the Durham team's work, one would also reasonably expect that relevant FISA information would be found in minimized form in the Page investigative file in Sentinel or in communications among FBI and NSD personnel responsible for that investigation, but the need for general access to the entire mass of Page FISA information retained in raw form on FBI storage systems has not been demonstrated. The Court, consequently, finds that use or disclosure of raw Page FISA information for the purpose of investigating or prosecuting potential crimes relating to the conduct of the Page or Crossfire Hurricane investigations is permissible only insofar as a particular need has been demonstrated to use or disclose specific information.

III. Conclusion

Neither the government nor the Court is free to depart from the plain meaning of §§ 1809(a)(2) and 1827(a)(2) simply to facilitate actions thought to be reasonable, or even laudable. With regard to reviewing the conduct of government personnel and prosecuting any criminal violations by them, the Court is permitting use or disclosure of information obtained from electronic surveillance or physical search of Page only where it has been or can be demonstrated to be necessary to remedy or deter the types of harm at which §§ 1809 and 1827 are addressed.

For the reasons stated above, IT IS HEREBY ORDERED as follows:

(1) With regard to the third-party FOIA litigation, see supra pp. 9-10, and the pending litigation with Page, see supra p. 12, the government may use or disclose Page FISA information insofar as necessary for the good-faith conduct of that litigation;

(2) With regard to any future claims brought by Page seeking redress for unlawful electronic surveillance or physical search or for disclosure of the results of such surveillance or search, the government may use or disclose Page FISA information insofar as necessary to the good-faith conduct of the litigation of such claims;

(3) Further use or disclosure of Page FISA information is permitted insofar as necessary to effective performance or disciplinary reviews of government personnel, provided that any such use or disclosure of raw information is permitted only insofar as a particular need to use or disclose the specific information at issue has been demonstrated. This paragraph applies, but is not limited to, use by, and disclosure by or to, the FBI's INSD or OPR;

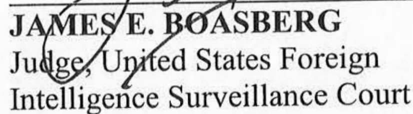
(4) Further use or disclosure of Page FISA information by DOJ OIG is permitted only insofar as necessary to assess the implementation of Recommendation 9 of the OIG Report;

TOP SECRET//SI//NOFORN/FISA

(5) Further use or disclosure of Page FISA information is permitted only insofar as necessary to investigate or prosecute potential crimes relating to the conduct of the Page or Crossfire Hurricane investigations, provided that any such use or disclosure of raw information is permitted only insofar as a particular need to use or disclose the specific information at issue has been demonstrated. This paragraph applies, but is not limited to, use by, and disclosure by or to, personnel engaged in the review being lead by United States Attorney Durham. See supra p. 17; and

(6) By January 29, 2021, and at intervals of no more than six months thereafter, the government shall submit under oath a written report on the retention, and any use or disclosure, of Page FISA information.

ENTERED this 25 day of June, 2020.



JAMES E. BOASBERG
Judge, United States Foreign
Intelligence Surveillance Court

I, [redacted], Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.

TOP SECRET//SI//NOFORN/FISA