UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

PASCAL ABIDOR, et al.	)	
Plaintiffs,	)	Civil Action No. 10 CV 4059
v.	)	
JANET NAPOLITANO, et al.	)	(Korman, J.) (Azrack, M.J.)
Defendants	)	

DEFENDANTS' REPLY TO PLAINTIFF'S SUPPLEMENTAL MEMORANDUM SUPPORTING EXPUNGEMENT OF GOVERNMENT RECORDS

Defendants submit this brief reply to address new arguments and to correct inaccurate statements made in Plaintiff's Supplemental Memorandum Supporting Expungement of Government Records Derived From Plaintiff Abidor's Private Digital Information ("Pl. Supp. Mem.").

1. In his supplemental memorandum, Plaintiff, for the first time, alleges that this Court's December 31, 2013 Memorandum and Order held that the two agency directives at issue[1] require the Government to destroy Government-created records containing descriptions of the contents of Plaintiff's laptop. *See* Pl. Supp. Mem. at 1 and 7. This belated argument misstates what the Court held in its earlier order. First, if this Court had so held, Plaintiff would have no reason to seek reconsideration, because the Court's Order would require the very relief he seeks in these supplemental submissions. Second, the portion of the Court's opinion that Plaintiff cites in support relates to the

[1] ICE Directive No. 7-6 (August 19, 2009) ("ICE Directive) and CBP Directive No. 3340-049 (August 20, 2009) ("CBP" Directive")

Court's inquiry at oral argument regarding whether Defendants would have destroyed the copy of the Plaintiff's laptop but for the filing of this case. Hr'g Tr., 32:2-9 (July 8, 2011). There was no inquiry by the Court or any statement by Defendants' counsel regarding the destruction of Government-created records that describe the contents of Plaintiff's devices.

2. In addition, Plaintiff's new contention that the Directives require the destruction of Government-created records documenting the search of his devices is also incorrect.[2] To support this new claim, Plaintiff cites to the provisions in the Directives discussing destruction of "copies of information from electronic devices." Pl. Supp. Mem. at 7-8 (citing to ICE Directive § 8.5(1)(e) and CBP Directive § 5.4.1.6). Plaintiff's reliance on those provisions is misplaced. As previously explained, the Directives (as well as the other related guidance cited by Defendants) distinguish between actual copies of information from electronic devices, on the one hand, and Government-created records related to the search maintained in an agency's system of records, on the other. *See* Defs. Supplemental Memorandum Regarding Defendants' Retention of Government Records (ECF Doc. 54) at 3-5. Plaintiff now attempts to avoid this distinction by suggesting that the term "copies of information" in the Directives should be interpreted so broadly as to include Government-created records describing the contents of an electronic device. Pl. Supp. Mem. at 8. This interpretation, however, ignores both Plaintiff's prior arguments in this litigation, as well as the plain language of the Directives. Plaintiff himself previously acknowledged the distinction between

[2] Plaintiff had not argued in any of his prior briefs that the Directives require destruction of Government-created records. Indeed, he argued just the opposite. Plaintiff argued that he had standing to challenge to the Directives because they permitted the retention of information from his electronic devices. *See* ECF Doc. 17 at 18.

"copies of his private digital information" (which he previously defined as "including both the images made from his electronic devices and all data copied or extracted from the devices or images"), and "government records derived from Plaintiff's digital files." ECF Doc. 46 at 6 and 10 (recognizing that while Rule 41(g) may be a vehicle for expungement of copies, it does not provide a vehicle for expungement of government records derived from Plaintiff's digital files).[3]

3. In addition, even if the language of the Directives regarding "copies of information" could be read so broadly as to include Government-created records containing "summaries" or "descriptions" of information found in a search of an electronic device, that reading conflicts with other provisions of the Directives that expressly permit CBP's and ICE's retention of information related to a search of electronic devices when such information is retained in a system of records consistent with otherwise applicable privacy and data protection rules. *See* ECF Doc. 54 at 5-6. In his memorandum, Plaintiff suggests that records related to border searches of electronic devices may be retained only if "the information at issue is specifically relevant to the agency's official duties, such as 'information collected in the course of immigration processing for the purposes of present and future admissibility of an alien.'" *See* Pl.

[3] Contrary to Plaintiff's contention, the Government's interpretation of the term "copy" to exclude Government-created records does not render the provisions requiring destruction of copies meaningless. *See* Pl. Supp. Mem. at 9. There is a clear distinction between a copy of all files on an electronic device and Government-created summaries describing particular files which were of interest to the Government during a search. Moreover, as previously explained, interpreting "copies of information" to exclude Government-created records is consistent with other provisions of the Directives. ECF Doc. at 4 n.4.

Supp. Mem. at 8-9 (quoting Section 5.4.1.2 of the CBP Directive).[4] But, as the language of the provision states, this is simply "an example," not a uniform limitation. *See, e.g.*, CBP Directive § 5.4.1.2 ("*For example*, information collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or ENFORCE or other systems as may be appropriate and consistent with the policies governing such systems.") (emphasis added). Moreover, Plaintiff's attempt to impute a requirement that any retained records be related to admissibility ignores the example cited in the corresponding section of the ICE Directive, which contains no such limitation. ICE Directive, § 8.5.1(b) ("information entered into TECS during the course of an investigation will be retained consistent with the policies").

4. Moreover, Plaintiff offers no valid justification for why investigative reports and other Government-created records relating to border searches of electronic devices should be treated any differently than investigative reports related to border searches of briefcases, suitcases, or other containers. Indeed, he cannot. In its Memorandum and Order, this Court rejected Plaintiff's claim that a border search of electronic devices should be treated any differently than a search of a suitcase. ECF 36 at 24-31. Thus, while some of the Government-created records relating to the search of Plaintiff's electronic device may contain information that Plaintiff may consider personal

[4] The systems of records in which the records at issue are maintained are not limited to records related to pending investigations. For example, ICE's External Investigative System of Records covers individuals who are the subject of "previous" law enforcement investigations and contain "investigative and evidentiary records" including "[i]ncident reports" and "[r]eports and memorandum prepared by investigators during the course of the investigation or received from other agencies participating or having information relevant to the investigation." 75 Fed. Reg. 404, 406 (Jan. 5, 2010).

or private, such records are no different — and are rightfully treated no differently — than incident and investigative reports relating to an inspection of a suitcase or a briefcase that may also make reference to personal or private items, but nonetheless are appropriately maintained by the Government in connection with its lawful exercise of its border search authority.[5]

5. Finally, Plaintiff's claim that the records at issue "seem to be broadly available throughout the Department of Homeland Security" (Pl. Supp. Mem. at 5) is also inaccurate. As Defendants have explained, the records at issue are subject to various restrictions: namely, the dissemination of the records is limited to personnel who have a "need to know" the information contained in the records for the performance of their official duties. *See* ECF Doc. 54 at 7-8.[6] Thus, contrary to Plaintiff's suggestion, the records at issue are not "widely available." Just like any other investigative reports, an employee would only have access to the records if he/she had a "need-to-know" the information for purposes of his/her official duties.[7]

---

[5] Plaintiff's contention that descriptions of the contents disclose "highly sensitive personal information" ignores the fact that many of the descriptions are similar in nature to Plaintiff's own publicly-available description of the contents of his laptop and the description in the Court's Memorandum and Order. *Compare* the description in Abidor_000001 to Abidor_000008, Abidor_000012 to Abidor_000016 with the descriptions in ECF Doc. 1, ¶ 32 and ECF Doc. 36 at 8, 31.

[6] Plaintiff suggests that Defendants have conceded that the records at issue are routinely available to front-line personnel who conduct primary and secondary inspections. Pl. Supp. Mem. at 5. This distorts the statement made by Defendants in their supplemental memorandum. The only document identified as being generally available to front-line personnel who conduct primary and secondary inspections was the TECS record (Abidor_000001), ECF Doc 58 at 7, which Plaintiff concedes that he is not challenging the Government's ability to retain. *See* Pl. Supp. Mem. at 8.

[7] This case is not analogous to *Lake v. Ehrlichman*, 723 F. Supp. 833, 834-35 (D.D.C. 1989), or *Smith v. Nixon*, 664 F. Supp. 601, 605 (D.D.C. 1987), where each court

For the foregoing reasons, Defendants respectfully request that the Court deny Plaintiff's Motion for Reconsideration.

Respectfully submitted,

LORETTA E. LYNCH
United States Attorney

ELLIOT M. SCHACHNER
Assistant U.S. Attorney

STUART F. DELERY
Assistant Attorney General

DIANE K. KELLEHER
Assistant Branch Director

s/Marcia Sowles
MARCIA SOWLES
Senior Counsel
U.S. Department of Justice, Civil Division
Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7114
Washington, D.C. 20530
Tel.: (202) 514-4960
Fax: (202) 616-8470
Email: marcia.sowles@usdoj.gov

---

exercised its equitable authority to order expungement of wiretap logs and summaries. In those cases, the court found that wiretaps were illegal. *Smith*, 664 F. Supp. at 602 (citing *Smith v. Nixon*, 807 F.2d 197, 204 (D.C. Cir. 1986) ("There is no dispute that the challenged wiretap was illegal (albeit not in violation of clearly established law)"); *Lake*, 723 F. Supp. at 834. This Court, in contrast, has already concluded that the search of Plaintiff's devices was lawful. Moreover, the Government's sole argument for the preservation of the records in those cases (*i.e.*, *Lake* and *Smith*) was that warrantless wiretaps initiated by the Nixon Administration "is *per se* a topic of historical interest." *Smith*, 664 F. Supp. at 604; *accord Lake*, 723 F. Supp. at 834. Here, the Government has articulated a number of reasons for the retention of the records at issue in this case. ECF Doc. 8-9.