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	)	

SUPPLEMENTAL MEMORANDUM REGARDING DEFENDANTS' RETENTION OF GOVERNMENT RECORDS

Plaintiff Pascal Abidor ("Plaintiff") has asked this Court to reverse its holding in its December 31, 2013 decision that he lacks standing. Specifically, Plaintiff claims that, despite the Court's analysis, he has standing because he "seeks expungement of all information unlawfully obtained from his devices, including data extracted or information derived from the contents of his devices or images." ECF Doc. 38-1 at 1 (emphasis deleted). As Defendants have previously represented, once this litigation is concluded, they will destroy any copies that they possess of Plaintiff's laptop or any other electronic devices, including all copies, if any, of data or files contained on his devices. The only records Defendants intend to retain are government-created records generated in connection with the search of Plaintiff's electronic devices, some of which contain descriptions of the contents of Plaintiff's laptop.

At the hearing on April 25, 2014, this Court ordered Defendants to (1) file under seal copies of "the summaries that were made of the records that were on [Plaintiff's] computer," (2) inform the Court as to any agency guidance, formal or informal,

interpreting the provisions of ICE Directive No. 7-6 (August 19, 2009) ("ICE Directive") and CBP Directive No. 3340-049 (August 20, 2009) ("CBP Directive") with regard the retention of such government-created records, and (3) inform the Court as to which of Defendants' personnel would have access to such documents and under what circumstances. Hr'g Tr. 36 - 39. The Court also provided Defendants an opportunity to review the hearing transcript and correct or clarify any statements made at the hearing. *Id.* at 24.

1. Description of Records Filed under Seal

Pursuant to the order, Defendants have filed under seal copies of those portions of the government-created records which they intend to retain that describe the contents of Plaintiff's computer. The material filed under seal consists of the following: (1) a sentence from CBP's TECS record of Plaintiff's border inspection (Abidor_000001), (2) a sentence from an entry made by ICE in TECS (Abidor_000002), (3) a sentence from an ICE incident report (Abidor_000003), (4) a sentence contained on two pages of an ICE Report of Investigation (Abidor_000004 to 000005), (5) a sentence contained on two pages of an ICE Report of Investigation (Abidor_000006 to 000007), (6) portions of a four page ICE Report of Investigation (Abidor_000008 to 000011), (7) a sentence contained on a page of an ICE Report of Investigation (Abidor_000012), (8) a sentence contained on two pages of an ICE Report of Investigation (Abidor_000013 to 000014), (9) a sentence contained on two pages of an ICE Report of Investigation (Abidor_000015

to 000016),[1] (10) portions of investigative summaries (Abidor_000017 to 000022), and (11) a portion of a page of an investigative summary (Abidor_000023).[2]

2. Interpretation of CBP and ICE Directives

Defendants' retention of government-created records describing items subject to lawful border searches, including electronic devices like Plaintiff's computer here, is not only usual and standard practice, but also is consistent with the plain language and purpose of the Directives. Both Directives specifically state that they do not limit the agencies' ability to record impressions or make reports related to border encounters. CBP Directive, § 2.3 (the Directive "does not limit CBP's ability to record impressions relating to border encounters"); ICE Directive, § 6.3 ("Nothing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems").

While the Directives provide for the destruction of "copies of information" from the electronic device searched, they do not refer to the destruction of government-created records related to the search (which was found lawful here) which may summarize or

[1] The sentence contained in Abidor_000002 is the same sentence contained in Abidor_00 0004 to 000008 and Abidor_000013-000016.

[2] As noted in Defendants' letter to the Court dated April 24, 2014 (ECF Doc. 50), in addition to the records created in connection with the border search, Defendants also possess litigation and briefing materials generated as a result of the filing of this lawsuit. These documents include memoranda and other communications among attorneys within the Department of Homeland Security ("DHS") and with attorneys at the Department of Justice, as well as internal briefing materials regarding this litigation. These non-operational documents, some of which are protected by the attorney-client and other applicable privileges, do not appear to be implicated by Plaintiff's motion and thus are not included in the material filed under seal. The retention of these materials is governed by the DHS General Legal Records Systems of Records, 76 Fed. Reg.72428 (Nov. 23, 2011).

describe information contained in the electronic device.[3] *See* CBP Directive, § 5.4.1.6 ("Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information"); § 5.3.1.2 ("Except as noted in section 5.4 or elsewhere in this Directive, if after reviewing the information . . . , there is not probable cause to seize it, any copies of the information must be destroyed, and any electronic device must be returned. Upon this determination that there is no value to the information copied from the device, the copy of the information is destroyed as expeditiously as possible, . . ."); ICE Directive, § 8.5.(1)(e) ("Copies of information from electronic devices, or portions thereof, determined to be of no relevance to ICE will be destroyed in accordance with ICE policy governing the particular form of information").[4]

In addition, the Department of Homeland Security has issued a Privacy Impact Assessment for the Border Searches of Electronic Devices ("PIA"), which provides further guidance. *See* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf. The PIA draws

---

[3] The word "copy" is defined as "something that is exactly like another." *Copy Definition,* Cambridge Dictionaries Online, http://dictionary.cambridge.org/us/dictionary/american-english /copy_3 (last visited May 15, 2014) ("to produce something that is exactly like another thing"); *Copy Definition,* Oxford Dictionaries, http://www.oxforddictionaries.com/us/definition/american_english/copy?9=copy (last visited May 15, 2014) ("a thing made to be similar or identical to another").

[4] Indeed, interpreting "copies of information" to exclude governmental records related to the search that describe the contents of the documents is also consistent with other provisions of the Directives. For example, Section 8.3 of the ICE Directive provides that "Special Agents are to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search." This provision would make no sense if "copies of information" was interpreted broadly to include government-created records describing the contents of the electronic devices.

a distinction between actual copies of information from electronic devices and government-created records related to the search which are maintained in an agency's system of records. The PIA provides:

> If a copy of data on a traveler's electronic device is made on-site and the device is returned to the traveler, a notation of the search is recorded in TECS. The copy is stored on either an ICE external hard drive or computer system, neither of which is connected to a shared or remote network; however, notes from the search may be stored in one of the systems of records listed below (*see* "[System of Records Notices]").

Id. at 8. In other words, government-created notes from a border search are stored in one of the systems of records. As explained *infra* at 6, the government-created records at issue are by definition the type of records included in one of the systems of records.

Moreover, even if the language in the CBP and ICE Directives regarding "copies of information" could be read to include government-created records containing "summaries" or "descriptions" of information contained in a searched electronic device, the Directives would nonetheless permit CBP and ICE to retain the government records at issue. Both the CBP and ICE Directives expressly provide that the agencies may retain information in their systems of records consistent with otherwise applicable privacy and data protection rules. The CBP Directive states that CBP may retain "information relating to immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained." CBP Directive, § 5.4.1.2. Similarly, the ICE Directive states that "ICE may retain information relevant to immigration, customs, and other law enforcement matters in ICE systems if such retention is consistent with the privacy and data protection policies of the system in which such information is retained."

ICE Directive, § 8.5.(1)(b). The government records at issue clearly fall within these provisions.

TECS, an updated and modified version of the former Department of Treasury Enforcement Communication Systems, is a system of records now principally owned and managed by CBP. *See* Notice of Privacy Act System of Records, 73 Fed. Reg. 77778 (Dec. 19, 2008). One of the purposes of this system is "to provide a record of any inspections conducted at the border by CBP." *Id.* at 77780-81. The TECS entry (Abidor_000001) is such a record: it provides a record of CBP's impressions and observations during the initial inspection of Abidor and his electronic devices, including his laptop.[5]

Nine of the other government records at issue here (Abidor_000002 to 000022) are maintained in ICE's External Investigations Systems of Records. *See* Notice of Privacy Act System of Records, 75 Fed. Reg. 404 (Jan. 5, 2010). This system of records covers individuals who are the subjects of "previous" law enforcement investigations, and contains various "investigatory and evidentiary records" including "[i]ncident reports" and "[r]eports and memoranda prepared by investigators during the course of the investigation or received from other agencies participating in or having information relevant to the investigation." *Id.* at 406.

The only other government record at issue (Abidor_000023) is covered by the DHS General Legal Records System of Records. *See* Notice of Privacy Act System of Records, 76 Fed. Reg. 72428 (Nov. 23, 2011).

[5] Retention of this document is also consistent with Section 5.4 of the CBP Directive, which permits an officer "to record impressions relating to border encounters."

3. Restrictions and Limitations on Access to Records

Access to records in these systems of records is strictly limited and subject to appropriate uses of the information. First, with respect to TECS, all records in TECS are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. "Access to TECS is controlled through a security subsystem, which is used to grant access to TECS information on a 'need-to-know' basis." 73 Fed. Reg. at 77781. Per DHS policy, DHS personnel have a "need-to-know" information if access is required for the performance of official duties. *See* Department of Homeland Security Management Directive 11042.1 at 1-2, (available at: https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf). For example, CBP personnel with a valid "need-to-know" would have access to Abidor_000001, including front-line personnel who conduct primary and secondary inspections.

In addition to the requirement that an employee has a "need to know" the information in order to perform their official duties, internal DHS access to TECS is controlled by CBP through the use of various safeguards including "using locks, alarm devices, and passwords, compartmentalizing databases, auditing software, and encrypting data communications." 73 Fed. Reg. at 77782. All users must also undergo a background investigation prior to being granted access. Privacy Impact Assessment for TECS System: CBP Primary and Secondary Processing ("TECS PIA") at 12 (available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf). In addition to this

threshold criterion for access, CBP also employs several layers of training, review and access control to ensure that information is accessed appropriately. *Id.*[6]

Second, with respect to ICE's External Investigations System of Records, access to ICE's External Investigations System of Records is similarly restricted. *See* 75 Fed. Reg. at 408. "Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions." *Id.* "Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated system security access policies." *Id.* at 408. To ensure against unauthorized access, "[t]he system maintains a real-time auditing function of individuals who access the system." *Id.*

Finally, access to the records in the DHS General Legal Records System of Records is also limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permission. 76 Fed. Reg. 72431. Records in this system are safeguarded in accordance with applicable rules and policies, including applicable DHS automated systems security and access policies. *Id.*

4. Clarifications of Statements Made at the April 25th Hearing

Defendants have reviewed the transcript of the hearing on April 25, 2014, and would like to clarify the statements made by counsel regarding the reasons for retaining

[6] The Privacy Act provides that "[n]o agency shall disclose any record which is contained in a system . . . to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains", except in certain circumstances such as disclosure to Congressional committees and sharing with other governmental agencies for law enforcement purposes, and 'routine uses' identified by an agency in its system of records notice. *See* 5 U.S.C. § 552a(b).

government-created documents. *See* Hr'g Tr. at 18, 22-23. Defendants note that they retain government-created records generated as a result of border searches not only to document the searches and for oversight, but also for law enforcement and homeland security purposes. *See, e.g.*, 73 Fed. Reg. at 77780-81 (purposes of TECS System of Records) (explaining that TECS contains records related to anti-terrorism and law enforcement); 75 Fed. Reg. at 407 (purposes of ICE –External Investigations System of Records) ("To identify potential criminal activity, immigration violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety.").

For the foregoing reasons, as well as those set forth in their prior filings, Defendants respectfully request that the Court deny Plaintiff's motion.

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