UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

PASCAL ABIDOR, *et al.* Plaintiffs, v. JANET NAPOLITANO, *et al.* Defendants.	Case No. 1:10-cv-04059 (Korman, J.) (Azrack, M.J.)

SUPPLEMENTAL MEMORANDUM SUPPORTING EXPUNGEMENT OF GOVERNMENT RECORDS DERIVED FROM PLAINTIFF ABIDOR'S PRIVATE DIGITAL INFORMATION

In its December 31, 2013 ruling, this Court held in relevant part that Plaintiff Pascal Abidor ("Plaintiff") does not have standing to seek expungement of information retained from his electronic devices, because the information he sought to have expunged would ultimately be destroyed. In so holding, the Court relied on Department of Homeland Security (DHS) Directives requiring the destruction of information obtained through border searches of travelers' electronic devices and on Defendants' representation that Plaintiff's "materials 'would have been destroyed but for the fact that cases had been filed,' and that they were being retained as potentially relevant to those cases." Mem. Op. & Order 20, ECF No. 36 (quoting Hr'g Tr., 32:4–29, June 8, 2011, ECF No. 25). When Plaintiff's counsel attempted to certify that his materials would be destroyed, however, Defendants' counsel stated only that Defendants would destroy images (i.e., complete copies) made of Plaintiff's laptop. Although Defendants now concede that they will destroy all copies made of Plaintiff's laptop and other electronic devices—including the data and files contained on those devices—they still refuse to destroy any records derived from

their search of Plaintiff's electronic devices. Moreover, they maintain that the Directives relied on by this Court in concluding that Plaintiff's information would be destroyed actually authorize the records' continued retention.

This Court should not countenance that result. As Plaintiff has consistently averred, Defendants' continued retention of his private information—whether in the form of copies made from his electronic devices or government records derived from the contents of those devices—qualifies as a continuing and unjustified invasion of his privacy. That invasion is particularly acute in this case, both because a significant portion of the records now at issue contain highly sensitive information, and because the records appear to be widely available on three separate DHS electronic databases. Previously, Defendants attempted to justify this significant intrusion on Plaintiff's privacy interests solely by arguing that the records are necessary to document agency activities. After prompting by this Court during oral argument, Defendants now assert a generalized law enforcement interest in retaining records created during the course of border search investigations; however, the mere hope that Plaintiff's private information may somehow prove relevant to some unspecified future investigation is insufficient to justify such a serious invasion of his personal privacy. Although Defendants argue that the CBP and ICE Directives regarding border searches of electronic devices authorize their continued retention of records derived from Plaintiff's private information, Defendants' proposed interpretation of the Directives would render the data retention protections contained therein utterly meaningless. Moreover, they provide no agency guidance to which the Court may defer on the question. For these reasons, the Court should uphold its initial determination that the Directives require expungement of Plaintiff's private information. If the Court concludes that the Directives do not require this result, it should order the records expunged pursuant to its equitable powers.

I. The Court Should Order Defendants To Expunge Records Derived from Their Search of Plaintiff's Electronic Devices.

A. Defendants' Continued Retention of Records Derived from Plaintiff's Electronic Devices Is a Serious and Ongoing Invasion of Plaintiff's Privacy.

As Plaintiff argued in his most recent memorandum, Mem. in Supp. of Pls.' Alt. Mot. for Relief Pursuant to Fed. R. Crim. P. 41(g) & for Expungement 10–13, ECF No. 46 ("Pls.' Rule 41(g) Mem."), equitable considerations require the expungement of government records derived from his private digital information, because Defendants' retention of this information long after any apparent need for it has dissipated qualifies as a significant and unjustified invasion of Plaintiff's privacy. *See Lake v. Ehrlichman*, 723 F. Supp. 833, 834–35 (D.D.C. 1989) (exercising the court's inherent equitable authority to order the expungement of wiretap logs, as well as FBI memoranda and summaries based the logs, because petitioners' privacy interests in their recorded conversation "clearly outweigh[ed] the interests of the government in preserving records of dubious interest and questionable accuracy"); *Smith v. Nixon*, 664 F. Supp. 601, 605 (D.D.C. 1987) (same). Individuals have a well-recognized privacy interest in the contents of their personal electronic devices. *United States v. Howe*, No. 09–CR–6076L, 2011 WL 2160472, at *7 (W.D.N.Y. May 27, 2011) (collecting cases). And Plaintiff's use of a password to secure his laptop, Abidor Decl. ¶ 5, ECF No. 47, further demonstrates his subjective expectation of privacy in the device's contents. *See Howe*, 2011 WL 2160472, at *7.

Plaintiff's significant privacy interest extends to all the files on his electronic devices, regardless of whether the files themselves contain apparently sensitive or mundane information, for at least two reasons. First, the Court is not well-positioned to determine what information will prove highly sensitive to Plaintiff—seemingly innocuous details may prove highly revealing or embarrassing in the context of Plaintiff's specific relationships. Second, government retention of

even mundane information qualifies as a significant dignitary harm. Most people would feel would feel "horrified," "offended," and "violated," to discover that the government was reading their diary or listening to their private conversations, *Smith*, 664 F. Supp. at 604, even if no especially sensitive information were disclosed. Thus, just as the courts in *Lake* and *Smith* did not parse the government's records of plaintiffs' private telephone conversations to determine whether any sensitive information was actually disclosed, this Court need not examine each individual government record to determine whether the information discussed seems mundane or highly sensitive.

Even if the Court disagrees that Plaintiff has a categorically strong privacy interest in the contents of his personal electronic devices, it is beyond dispute that many of the records at issue here disclose a significant amount of highly sensitive personal information. [redacted] Numerous other files mentioning Plaintiff's possession of images and news stories relating to his Islamic Studies research, including images of Hezbollah fighters, could potentially prove immensely prejudicial

[1] [redacted]

in future encounters with government officials. *See Paton v. La Prade*, 524 F.2d 862, 868 (3d Cir. 1975) ("[H]istory of a not too distant era has demonstrated that future misuse of a file labeled 'Subversive Material' can prove extremely damaging. As the district court aptly observed, 'the existence of (the) records may at a later time become a detriment to [the plaintiff].'").[2]

The harm occasioned by Defendants' unjustified retention of records describing Plaintiff's information is exacerbated in this case by the fact that the records themselves seem to be broadly available throughout the Department of Homeland Security. At the April 25 hearing, Defendants repeatedly stated that the records at issue here would not be accessible to agents conducting routine inspections at the border. Hr'g Tr. 19:6–20:6, Apr. 25, 2014. Now, however, they concede that the records are available to DHS personnel who have a "need-to-know" the information contained in the records for the performance of their official duties, "including front-line personnel who conduct primary and secondary inspections." Supplemental Mem. Regarding Defs.' Retention of Gov't Records 7, ECF No. 54.[3]

The records at issue here are apparently stored in three separate DHS databases: the Department of Treasury Enforcement Communication Systems (TECS) database, *see* Notice of Privacy Act System of Records, 73 Fed. Reg. 77,778 (Dec. 19, 2008), which is now primarily managed by CBP; the External Investigations Systems of Records, *see* Notice of Privacy Act System of Records, 75 Fed. Reg. 404 (Jan. 5, 2010), run by U.S. Immigration and Customs

[2] To be sure, in some circumstances the government might legitimately claim some law enforcement interest in retaining such records. But, as discussed further below, Defendants claim no law enforcement interest in the specific records at issue here, presumably because Plaintiff's academic work in Islamic Studies fully explains his possession of these images.

[3] *See also* 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.

Enforcement (ICE); and DHS's General Legal Records System of Records, *see* Notice of Privacy Act System of Records, 76 Fed. Reg. 72,428 (Nov. 23, 2011). Defendants point out that internal DHS access to the TECS database is controlled through the use of "locks, alarm devices, and passwords, compartmentalizing databases, auditing software, and encrypting data communications," 73 Fed. Reg. 77,782, and that all users of the database must undergo a background investigation prior to obtaining access to the database.[4] Even assuming these safeguards work entirely as intended, Plaintiff's information remains officially available to border officials screening him for entry every time he enters the United States. Moreover, although Defendants state that the other two databases are "similarly restricted," they provide almost no information regarding who may actually access these databases to view Plaintiff's private information. Instead, they merely assert that the records are "safeguarded in accordance with applicable rules and policies." Supplemental Mem. Regarding Defs.' Retention of Gov't Records 8 (citing 75 Fed. Reg. at 408; 76 Fed. Reg. at 72,431). Far from the proverbially secure lockbox, it appears that Plaintiff's private information is widely available on numerous government databases.

B. Defendants Have Failed to Identify Any Significant Governmental Interest Justifying Retention of Plaintiff's Private Information.

Until recently, Defendants attempted to justify their retention of records based on Plaintiff's private information solely on the ground that the records were necessary for purposes of documenting and reviewing agency activities. *See* Defs.' Opp'n to Pls.' Mot. for Recons. 6, ECF No. 39; Defs.' Supplemental Mem. 6, ECF No. 45; Hr'g Tr. 18:12–20, Apr. 25, 2014 ("[I]t's a government record that's retained solely for . . . government purposes to document, you

[4] *See* Privacy impact Assessment for TECS System: CBP Primary and Secondary Processing 12, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf.

know, what they did . . . . [I]t's retained . . . solely for – you know, to document what the government did . . for oversight purpose[s]."). Now, after prompting by the Court at oral argument, Defendants assert 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." Supplemental Mem. Regarding Defs.' Retention of Gov't Records 8–9. Defendants' new reliance on this generalized law enforcement interest provides no more justification for their continued retention of Plaintiff's private information than their initial interest in documentation. As the Sixth Circuit made clear in *Sovereign News Co. v. United States*, the government may not hold onto an innocent party's private files and information "purely for the sake of keeping them or because it is 'hopeful' that they may be relevant to some future investigation. This amounts to harassment." 690 F.2d 569, 577 (6th Cir. 1982).

Additionally, Defendants argue that the CBP and ICE Directives regarding border searches of electronic devices—ICE Directive No. 7-6.1 (August 18, 2009) ("ICE Directive") and CBP Directive No. 3340-049 (August 20, 2009) ("CBP Directive")—authorize their continued retention of Plaintiff's private information. Supplemental Mem. Regarding Defs.' Retention of Gov't Records 3–6. But the documents themselves provide no such authorization. To the contrary, as this Court reasoned in its December 31, 2013, Memorandum and Order, the Directives compel the destruction of all materials containing Plaintiff's private information, whatever form those materials might take. *See* Mem. & Order 20 ("[U]nder the regulations [Plaintiff] is entitled to have the materials destroyed."); 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.");

CBP Directive § 5.4.1.6 ("Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probably cause to seize the information, CBP will retain no copies of the information.").

To escape this plain language, Defendants attempt to construe other provisions of the Directives to authorize their retention of records based on Plaintiff's private information. Defendants point first to provisions stating that the Directives do not limit officials' ability to "record impressions relating to border encounters." CBP Directive, § 2.3; *see also* 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."). These provisions are inapposite. Plaintiff has repeatedly made clear that he is not challenging Defendants' initial decision to record information relating to his border incident. Rather, he seeks only the destruction of records derived from Defendants' forensic review of the contents of his electronic devices.

Defendants also assert that the Directives authorize retention of the records in this case, because they allow ICE and CBP to 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; ICE Directive § 8.5(1)(b). These provisions, however, cannot mean that *any* information obtained pursuant to a border search of a traveler's electronic device may be retained indefinitely. Such a reading would negate the provisions requiring ICE and CBP to destroy information once it has become clear that it is no longer relevant to the agencies' duties. *See* ICE Directive § 8.5(1)(e); CBP Directive § 5.4.1.6. Rather, the provisions appear to contemplate allowances for database retention only where 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." CBP Directive § 5.4.1.2.[5]

Finally, Defendants argue that the requirement to destroy "copies" of information does not extend to derivative government records, because the records are not identical to the information they purport to describe. Again, however, Defendants' proposed interpretation would render the Directives' retention protections meaningless. What would it matter that DHS must destroy copies of information for which it no longer has any specific, legitimate use, if it could indefinitely retain records describing that same information? This Court should not construe the Directives in a manner that so directly contravenes their plain intent.

Moreover, Defendants' interpretations of the above-cited provisions, for which they cite no applicable agency authority, are not entitled to deference under *Auer v. Robbins*, 519 U.S. 452 (1997). As the Supreme Court explained in *Christopher v. SmithKline Beecham Corp.*, *Auer* deference is inappropriate where the agency interpretation is "nothing more than a convenient litigating position, or a *post hoc* rationalizatio[n] advanced by an agency seeking to defend past agency action against attack." 132 S. Ct. 2156, 2166–67 (2012) (citations and internal quotation marks omitted) (alteration in original). Defendants presumably recognize that there are no agency interpretations of the Directives to which the Court may accord *Auer* deference, because they do not event attempt to invoke it in their papers, notwithstanding this Court's instruction to

[5] DHS's Privacy Impact Assessment for the Border Searches of Electronic Devices, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf, reinforces this limited interpretation of the agency's authority to indefinitely retain records derived from border searches of travelers' electronic devices. *See id.* at 8 ("[N]otes from the search may be stored in one of the systems of records listed below (see 'SORNs'). For example, information found on the electronic devices that pertains to the traveler's admissibility may be noted in ENFORCE.").

provide an authoritative agency interpretation if one is available. *See* Hr'g Tr. 20:7–24, 37:1–5, Apr. 25, 2014.

Nevertheless, even if the Court agrees with Defendants that the Directives do not *require* the expungement of the records at issue here, they certainly do not authorize or otherwise support Defendants' continued retention of Plaintiff's private information. For that reason, the Court should exercise its inherent equitable powers to remedy the serious and ongoing invasion of Plaintiff's privacy.

CONCLUSION

For the foregoing reasons, the Court should order Defendants to expunge all government records derived from the border search of Plaintiff's electronic devices. If, however, the Court concludes that Defendants need not expunge all the records at issue here, it should reconsider its December 31, 2013, ruling to the extent that it dismissed Plaintiff Abidor's claims for lack of standing.

Respectfully submitted,

/s/ Brian M. Hauss
Brian M. Hauss
Catherine Crump
Hina Shamsi
American Civil Liberties Union Foundation
125 Broad St., 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2583
Email: bhauss@aclu.org

Mason C. Clutter
National Association of Criminal Defense Lawyers
1660 L Street, N.W., 12th Floor
Washington, D.C. 20036
(202) 465-7658

Christopher Dunn
Arthur Eisenberg
New York Civil Liberties Union Foundation
125 Broad St., 19th Floor
New York, NY 10004
(212) 607-3300