UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. U.S. CUSTOMS AND BORDER PROTECTION, Defendant.	)	Civil Action No: 14-1217 (RBW)

DEFENDANT'S REPLY IN SUPPORT OF MOTIONFOR SUMMARY JUDGMENT AND OPPOSITION TO PLAINTIFF'S CROSS-MOTION FOR SUMMARY JUDGMENT

INTRODUCTION

The final issue in this case concerns whether U. S. Customs and Border Protection (CBP) properly asserted Exemption 7(E) of FOIA in withholding Analytical Framework for Intelligence (AFI) training materials, statements of work, and other documents; in addition, plaintiffs question the reasonableness of CBP's segregation of released materials. Plaintiff Electronic Privacy Information Center (EPIC) specifically focuses on two sub-requirements under Exemption 7(E): (1) whether the withheld materials pertain to "techniques and procedures" for "law enforcement investigations and prosecutions," and (2) whether these materials "could reasonably be expected to risk circumvention of the law."

ARGUMENT

A. Records Withheld by CBP Encompass Techniques and Procedures for Law Enforcement Investigations or Prosecutions

This Court recently addressed the general standard courts must bring to bear in analyzing agency assertions of Exemption 7(E). *See Long v. ICE*, --- F. Supp. 3d ---, 2015 WL 8751005, at *5 (D.D.C. Dec. 14, 2015). The Court in *Long* held that "Exemption 7(E) sets a relatively low bar for the agency to justify withholding, *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011), and where an agency specializes in law enforcement, its decision to invoke [E]xemption 7 is entitled to deference, *Lardner v. DOJ*, 638 F. Supp. 2d 14, 31 (D.D.C. 2009) (quoting *Campbell v. DOJ*, 164 F.3d 20, 32 (D.C. Cir. 1998)." *Id.* The agency has more than met its burden in this case.

In their Opposition and Cross-Motion, EPIC places heavy emphasis on a phrase from the District Court in *EPIC v. DHS*, asserting that Exemption 7(E) pertains "only to acts by law enforcement after or during the commission of a crime." 999 F. Supp. 2d. 24, 31 (D.D.C. 2013) rev'd on grounds of Exemption 7(F) by *EPIC v. DHS*, 777 F.3d 518 (D.C. Cir. 2015). This emphasis is understandable, as the court's language appears to strictly limit the scope of 7(E). However, the District Court in *EPIC* failed to cite any authority to support its assertion. This is unsurprising, as even EPIC's own motion cites several cases directly undermining the District Court's statement. *See* EPIC MSJ at 6. For example, EPIC cites *Henderson v. Office of the Director of National Intelligence*, which upheld the non-disclosure of "background checks," as well as *CREW v. DOJ*, upholding the non-disclosure of "the operational capabilities of unmanned drones." *See id.* (citing *Henderson*, --- F. Supp. 3d ---, 2016 WL 755608, at *1 (D.D.C. 2016), and *CREW*, --- F. Supp. 3d ---, 2016 WL 541127, at *12 (D.D.C. 2016)). Neither background checks nor the operational capabilities of unmanned drones necessarily pertain to "acts by law enforcement after or during the commission of a crime," yet their non-disclosure

was upheld under Exemption 7(E). The same can be said of "computer codes relating to a law enforcement database," "details on how a law enforcement database is searched, organized, and reported," and "the type of surveillance equipment [used] or the location and timing of its use." *See id.* (citing *Strunk v. Dep't of State*, 905 F. Supp. 2d 142, 148 (D.D.C. 2012), *Blackwell v. FBI*, 680 F. Supp. 2d 79, 92 (D.D.C. 2010), *aff'd* 646 F.3d 37 (D.C. Cir. 2011), and *Showing Animals Respect and Kindness v. Dep't of the Interior*, 730 F. Supp. 2d 180, 200 (D.D.C. 2010) (internal quotation marks omitted)). Finally, as noted above, *EPIC v. DHS* was reversed on appeal under Exemption 7(F). *See* 777 F.3d at 520. The D.C. Circuit explicitly left unaddressed the district court's conclusions regarding Exemption 7(E). *See id.* at 528.

Moreover, investigative techniques by their nature involve procedures to be implemented in the absence of U.S. law: to wit, sometimes investigations happen on suspicion of a violation that did not, in fact, occur, or are initiated to prevent violations from occurring. As explained in the Supplemental Burroughs Declaration, AFI "enhances DHS' ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk." Supp. Decl. at ¶ 8. The emphasis is on investigating "potential" law enforcement or security risks to identify persons who may seek to violate U.S. law. Just because the violation or the risk is potential, does not render the actions of law enforcement officers and agents any less investigatory. By analogy, local police are often called upon, while patrolling, to determine whether a violation of law has occurred or is in progress, or to act proactively to prevent crimes from occurring. Techniques and procedures used to prevent the violation of U.S. law, or determine whether a violation has occurred or is in progress would almost certainly qualify as law enforcement techniques and procedures. This is even clearer in the context that CBP is working in because CBP is seeking to prevent, for example, "terrorists, their weapons, and other dangerous items

from entering the United States." *Id.* at ¶ 9 (emphasis added). In other words, CBP must constantly investigate whether a person or shipment poses a risk of violating U.S. law, considering both past activities—when incorporating past information to detect "trends, patterns, and emerging threats," *id.*—and present because the best opportunity to stop a terrorist or other criminal, or dangerous items, from entering the United States, is before such person enters the country or boards transportation at a foreign port, or a shipment arrives in the U.S. or is loaded onto a conveyance destined for the U.S. Holding that such activities qualify as law enforcement investigatory procedures and techniques would not lead to an impermissible expansion of Exemption 7(E). CBP is constantly investigating (referred to as "vetting") incoming travelers and cargo in order to detect persons or shipments which may violate U.S. law or seek to engage in activities which violate U.S. law. These procedures are exactly the sort of techniques that law enforcement organizations implement regularly to prevent violations of law from occurring, or if they occur, to determine by whom, how and why; with the goal of taking enforcement action against the culprit, but also to prevent such activities from being taken in the future.

CBP is not seeking to withhold, as EPIC implies, "mere logistical details." EPIC MSJ at 8 (quoting *Clemente v. FBI*, 741 F. Supp. 2d 64, 88 (D.D.C. Sept. 28, 2010) (internal quotation marks omitted)). CBP is instead withholding documents in order "to protect investigatory techniques whose disclosure could result in evasion of arrest or other enforcement actions." 741 F. Supp. 2d at 88. The *Clemente* court was concerned that the FBI had not produced enough evidence from which the court could "deduce something of the nature of the techniques in question." *Id.* Here, in contrast, the nature of the techniques in question is clear: they are methods used to assess potential criminal risk of individuals and shipments seeking to enter the United States to aid in the enforcement of U.S. law at the border.

Courts in this district have frequently and consistently upheld non-disclosure of seemingly innocuous data and practices, implying that such data and practices qualify as more than "mere logistical details." Non-disclosure under Exemption 7(E) has been upheld for "the manner in which . . . data is searched, organized and reported to the FBI," *Blackwell*, 646 F.3d at 42, computer screen transaction codes, *see Strunk*, 905 F. Supp. 3d at 148, "violator identifier codes," *Ortiz v. DOJ*, 67 F. Supp. 3d 109, 123 (D.D.C. 2014), and "codes relate[d] to procedures concerning the use of law enforcement resources and databases," *Miller v. DOJ*, 872 F. Supp. 2d 12, 29 (D.D.C. 2012). *See also*, *Skinner v. DOJ*, 893 F. Supp. 2d 109, 114 (D.D.C. 2012) and *Long*, 2015 WL 8751005 at *6. This line of cases suggests not only the general deference courts bring to analysis under Exemption 7, *see Campbell*, 164 F.3d at 32, but also an understanding that persons seeking to violate U.S. law could use disclosed information that on its face seems harmless, to then develop and "employ countermeasures to avoid detection," *Blackwell*, 646 F.3d at 42 (quoting Chief of the FBI's Record/Information Dissemination Section) (internal quotation marks omitted). Such countermeasures are exactly what concerns CBP here.

EPIC concedes that the withheld documents "may contain information that assists CBP agents in their daily screening tasks," but EPIC goes on to suggest that so too would training for "Microsoft Word" or a "coffee machine." EPIC MSJ at 9. The implication appears to be that training on using AFI has too attenuated a connection to law enforcement techniques and procedures to qualify for non-disclosure under 7(E). However, in this instance, information that assists CBP officers and agents in the daily tasks at issue is exactly the sort of information CBP uses to detect potential violations of law at the border. One way to tell is to ask whether a criminal could make use of AFI training for "daily screening tasks" to develop and "employ countermeasures to avoid detection" in a way that the criminal could not make use of

"instructions on how to use a coffee machine." The answer is clear, and so is the justification for non-disclosure.

B. Disclosure of Records Currently Withheld by CBP Could Reasonably Be Expected to Risk Circumvention of the Law

CBP has far surmounted the "relatively low bar" courts impose when conducting a 7(E) analysis. *Blackwell*, 646 F.3d at 42. Broadly, the two main concerns of CBP are (1), as was discussed above, the possibility that persons seeking to violate U.S. law could use knowledge of CBP targeting and other law enforcement techniques to avoid being detected by those same techniques and (2) the risk that knowledge of encryption standards and methods could facilitate the same sort of evasion or a possible cyber-attack on CBP's systems. In its previous Opinion, this Court noted without deciding "that the Burroughs Declaration may establish the risk of circumvention of law, assuming that the withheld information about the AFI system would indeed disclose law enforcement techniques or procedures for investigations or prosecution." ECF No. 28 at 5. This Court repeated the D.C. Circuit's guidance that Exemption 7(E)

> looks not just for circumvention of the law, but for a risk of circumvention; not just for an actual or certain risk of circumvention, but for an expected risk; not just for an undeniably or universally expected risk, but for a reasonably expected risk; and not just for certitude of a reasonably expected risk, but for the chance of a reasonably expected risk.

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

EPIC specifically takes issue with three of the risks identified in the Supplemental Burroughs Declaration: CBP's arguments that disclosure of (1) AFI screenshots would allow bad actors to more easily access, manipulate, extract information from and otherwise affect or destroy data contained on CBP computer systems; (2) LexisNexis products could reveal methods by which data is searched, organized and reported; and (3) encryption standards used to protect the security of the database could allow criminals to bypass such protections. *See* EPIC MSJ at

8-11 and Supp. Burroughs Decl. at ¶¶ 11-16. EPIC asserts that the AFI documents would not provide a detailed roadmap for bad actors "unless those bad actors are training for a job at CBP." EPIC MSJ at 9. But training provided to officers and agents seeking to prevent and interdict criminals and contraband entering the country seems exactly the sort of material that would risk circumvention of the law if disclosed. EPIC then calls "incredible and logically deficient" the claim that knowledge of the system's interface would facilitate criminal interference with the system. *Id.* at 9. However, while knowledge of the coding providing the infrastructure of the system would be *more* helpful to a criminal, there is enough reason to believe that understanding the organization of the system and of the data stored thereon would risk circumvention of the law.

As for the Lexis products, EPIC argues that Ms. Burroughs failed to describe "why or how the work orders would describe search terms, methods of organizing data, or how data is reported to CBP or other agencies." EPIC MSJ at 10. But it is enough that the work orders do describe details that "could reasonably allow a person to recognize search terms specifically applied by law enforcement to query LexisNexis databases." Supp. Burroughs Decl. at ¶ 16. Such recognition of search terms, along with a sense of data organizing and reporting, is enough to risk circumvention of law. Exactly "why or how" the work orders describe such queries or methods of organizing data is not necessary because the above already provides a "sufficiently specific link" between the materials withheld and the risks of disclosure. *Island Film, S.A. v. Dep't of the Treasury*, 869 F. Supp. 2d 123, 138 (D.D.C. 2012). As for the encryption standards, while EPIC is correct that publications such as the Department of Commerce's guidelines[1] exist and are public, CBP is not required to release the specific encryption standards it has opted to

[1] Elaine Barker, Nat'l Inst. for Standards and Technology, U.S. Dep't of Commerce, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, Special Pub. No. 800-175B (Mar. 2016).

use. The Department of Commerce's guidelines discuss a vast variety of cryptographic algorithms, keys, cryptographic services, and organizations that publish standards for data security. Publishing the Department of Commerce guide is a far cry from disclosing any specific details or general approaches of specific systems used by an agency.

Finally, a flaw runs through all three attacks on CBP's arguments: EPIC has failed to provide even general evidence as to why the risks identified by CBP do not exist or are *de minimis*. An excellent guide to what this might look like comes from the plaintiffs in *Long*. *See* 2015 WL 8751005 at *8. The plaintiffs in that case "aggressively challenged Defendants' assertion that disclosure . . . would expose the . . . databases to a SQL injection attack." *Id.* (*see id.* at *7 for a description of a SQL injection hack). The plaintiffs provided a declaration from "an expert in data security" who explained that such an attack was "not a credible threat" based on the facts of the case. *Id.* at *8 (internal quotation marks omitted). (The court in *Long* permitted the defendants to supplement the record with additional evidence. *Id.* at *10). The logic of *Long* is not mysterious or surprising. If EPIC wants to call CBP's arguments about risk into question, it cannot simply assert that disclosure "could not plausibly create a risk of circumvention of the law." EPIC MSJ at 11.

C. The Agency Satisfied the Segregability Requirement

The final issue EPIC presses is that of segregability, arguing that "CBP has failed to meet its burden." EPIC MSJ at 12. EPIC's arguments fail to take account of the precedent in this Circuit. "The question of segregability is by necessity subjective and context-specific," *Schoenman v. FBI*, 763 F. Supp. 2d 173, 202 (D.D.C. 2011), and an agency need not "commit significant time and resources to the separation of disjointed words, phrases, or even sentences which taken separately or together have minimal or no information content," *id.* (quoting *Mead*

Data v. Dep't of the Air Force, 566 F.2d 242, 261 n.55 (D.C. Cir. 1977) (internal quotation marks omitted)). CBP, through its *Vaughn* index, has described the categories of information withheld, and the segregation section of FOIA, § 552(b), does not require disclosure of bits and pieces of records that would provide little information. *See Nat'l Sec. Archive Fund, Inc. v. CIA*, 402 F. Supp. 2d 211, 220-21 (D.D.C. 2005). Courts "may rely on government affidavits that show with reasonable specificity why documents withheld pursuant to a valid exemption cannot be further segregated." *Juarez v. Dep't of Justice*, 518 F.3d 54, 61 (D.C. Cir. 2008) (citation omitted). Here, the agency has met its burden by providing a reasonably detailed justification, which need not be so detailed as to compromise the nature of the withheld information. *Mead Data*, 566 F.2d at 261. Considering the precedents of this Circuit, CBP has met its segregability burden under FOIA.

CONCLUSION

For the foregoing reasons, the Court should enter judgment in favor of the Defendant and deny Plaintiff's cross-motion for summary judgment.

Respectfully submitted,

CHANNING D. PHILLIPS , DC Bar # 415793
United States Attorney for the District of Columbia

DANIEL F. VAN HORN, DC Bar # 924092
Chief, Civil Division

PATRICIA K. MCBRIDE, PA Bar # 54561
Assistant United States Attorney
Civil Division
555 4th Street, NW, Room E-4808
Washington, DC 20530
Tel: 202.252.7123

Fax: 202.252.2599
Email: patricia.mcbride@usdoj.gov

Attorneys for Defendant

CERTIFICATE OF SERVICE

I certify that I caused a copy of the foregoing Reply Motion for Summary Judgment will be electronically served, on this 30th day of June, 2016 by CM/ECF upon counsel for Plaintiff.

_____

PATRICIA K. MCBRIDE, PA Bar # 54561
Assistant United States Attorney