Knight First Amend. Inst. at Columbia Univ. v. Dep't of Homeland Sec.
No. 1:17-cv-00548-TSC

Defendants' Combined Reply in Support of Their Motion for Summary Judgment and Opposition to Plaintiff's Cross Motion for Summary Judgment

Ex. B

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY, Plaintiff, v. DEPARTMENT OF HOMELAND SECURITY, *et al.*, Defendants.	)	No. 1:17-cv-00548-TSC

DECLARATION OF PATRICK A. HOWARD

I, Patrick A. Howard, declare as follows:

1. I am a Branch Chief in the Freedom of Information Act (FOIA) Division, Privacy and Diversity Office, Office of the Commissioner, U.S. Customs and Border Protection (CBP). I have been a Branch Chief in the FOIA Division in Washington, D.C. since February 8, 2015. In this capacity, I oversee a staff of Government Information Specialists, the processing of requests for records submitted to CBP pursuant to the FOIA, the processing of certain requests submitted to CBP pursuant to 5 U.S.C. § 552, the Privacy Act, 5 U.S.C. § 552a, and other activities conducted pursuant to applicable records access provisions.
2. I am familiar with CBP's procedures for responding to FOIA requests. I provide technical and administrative supervision and direction to a group of Government Information Specialists responsible for processing requests for release of CBP documents and information, assist with FOIA litigation matters, and I am personally

familiar with the processing of FOIA responses, including, at times, by directly reviewing for adequacy and compliance with federal laws and regulations.

3. All information contained herein is based upon information furnished to me in my official capacity, and the statements I make in this declaration are based on my personal knowledge, which includes knowledge acquired through, and agency files reviewed in, the course of my official duties as Branch Chief in CBP's FOIA Division.

4. The purpose of this declaration is to provide additional information as to why certain information was withheld from public disclosure pursuant to 5 U.S.C. §§ 552 (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E) in support of the Government's motion for summary judgment submitted in this case.

PLAINTIFF'S REQUEST TO CBP

5. I am familiar with Plaintiff Knight First Amendment Institute at Columbia University's (hereinafter Plaintiff) FOIA request for information from CBP that was received by the CBP FOIA Office on March 24, 2017. I am also familiar with the Plaintiff's allegations in this litigation.

    a. In its request, Plaintiff requested the following:

        1. Any document containing statistical information concerning the search, detention, retention, or sharing of electronic devices or information of individuals at the border (or functional equivalent of the border) since FY2012, including, but not limited to, documents reflecting:

            a. The number of travelers whose electronic devices or information were searched, detained, retained, or shared;

b. The number or portion of those travelers who are U.S. citizens;

c. The number or portion of those travelers who are lawful permanent residents or green card holders;

d. The number or portion of those travelers by country of origin;

e. The number or portion of those travelers by gender, race, ethnicity, nationality, and/or country of birth;

f. The number or portion of those travelers by port of entry; and

g. The number or portion of those travelers by watch list, lookout, and/or other selectee status.

2. Documents relating to each instances since FY2012 in which CBP or ICE searched, detained, retained, or shared an electronic device or the information accessible on it, including, but not limited to:

a. A list of the TECS data field categories used to record and track each electronic device conducted by CBP or ICE; and

b. All information contained in the TECS system used to record and track electronic device searches, detentions, retentions, and/or sharings.

3. Revisions of or documents supplementing or superseding:

a. CBP Directive No. 3340-049, *Border Search of Electronic Devices Containing Information* (Aug. 20, 2009); or

b. ICE Directive No. 7-6.1, *Border Searches of Electronic Devices* (Aug. 18, 2009).

4. The following documents relating to any reviews of CBP's or ICE's policies or practices concerning electronic device searches;

    a. Any audits, impact assessments, or other reviews of CBP's or ICE's policies or practices concerning electronic device searches, including any such reports by the Office for Civil Rights and Civil Liberties, DHS's OIG, and CBP's Office of Internal Affairs, Management Inspection Division;

    b. Any policies, practices, procedures, and/or training materials adopted as a result of any audits, impact assessments, or other reviews of how CBP and ICE conduct electronic device searches; and

    c. Any documents reflecting annual or semi-annual examinations by CBP or ICE of electronic device searches by port of entry, as adopted in response to the 2011 Impact Assessment.

5. Documents, including tear sheets and TRIP records, containing or relating to complaints filed by individuals or organizations about CBP's and/or ICE's search, review, retention or sharing of the information on travelers' electronic device.

6. Documents reflecting policies, practices, or procedures concerning how CBP officers handle "privileged or other sensitive material," including "work-related information carried by journalists," as referenced in § 5.2 of the CBP Directive.

7. Documents reflecting policies, practices, and procedures concerning CBP's anti-discrimination policy as applied to discretionary device searches.

CBP'S RESPONSE TO PLAINTIFF'S REQUEST

6. In response to Plaintiff's Request, CBP has provided 4,185 partially released pages (*i.e.*, pages in which portions were withheld pursuant to an applicable exemption), withheld 2 pages in their entirety, and determined that 106 pages were not responsive. Additionally, consistent with an agreement with Plaintiff, CBP produced a 1,424-page spreadsheet of information. In addition, CBP processed 47 pages of records referred to CBP by TSA, all of which were partially released. In addition, CBP processed 1,285 pages of records referred to CBP from DHS.
7. On January 31, 2020, CBP provided a Vaughn Index and Declaration, included with Defendant's Motion for Summary Judgment.

JUSTIFICATION FOR WITHHOLDING INFORMATION UNDER FOIA

CBP Withheld Pre-decisional, Deliberative Information Pursuant to Exemption (b)(5)

8. In CBP's March 15, 2019 release, CBP provided Plaintiff with 282 pages of partially redacted records and identified another 311 pages that CBP withheld in full. As described in CBP's *Vaughn* index, which was attached to my January 30, 2020 Declaration in this case, the 282 pages of records released with partial redaction consist

of materials obtained, compiled, or created by the DHS Office of Civil Rights and Civil Liberties (CRCL) in relation to their review of CBP law enforcement activities, including activities relating to border searches of electronic devices. Pursuant to 5 U.S.C. § 552(b)(5), CBP redacted from the records information subject to the deliberative process privilege – more specifically, "[i]nformation regarding the pre-decisional status of an internal review or investigation and the methods used to conduct such review or investigation, the disclosure of which would reveal deliberative, pre-decisional information regarding the agency decision-making process." *CBP Vaughn* at 23.

9. The March 15, 2019 release letter also advised Plaintiff that 311 pages were withheld in their entirety. As set forth in CBP's *Vaughn* index, 271 pages consisted of spreadsheets detailing border searches of electronic devices and related statistical analysis. *Id.* at 27-30. The information was withheld, in part, under 5 U.S.C. § 552(b)(5) due to the inclusion of information compiled and analyses conducted to support recommendations to agency leadership. *Id.* at 28. The records also included substantial amounts of information that were exempt under § 552(b)(6), (b)(7)(C), and (b)(7)(E).

10. Like the rest of the records addressed in CBP's March 15, 2019 release letter, the 271 pages of spreadsheets and related statistical analysis withheld by CBP were obtained, compiled, or created by CRCL in relation to their review of CBP law enforcement activities, including activities relating to border searches of electronic devices. The CBP information in the documents was disclosed to inform CRCL's review and analysis of CBP activities.

11. CRCL's responsibilities include, among other things, "promoting respect for civil rights and civil liberties in policy development . . . ." Declaration of James V.M.L. Holzer in Support of Defendants' Motion for Summary Judgment, at 2-3, ¶ 10(a)-(b) (Jan. 31, 2020). On December 29, 2011, CRCL issued an Impact Assessment regarding border searches of electronic devices. CRCL Impact Assessment, Border Searches of Electronic Devices, *available at* https://www.dhs.gov/sites/default/files/publications/crcl-border-search-impact-assessment_06-03-13_1.pdf. CRCL's review stemmed from ICE's and CBP's August 2009 issuance of revised policies governing border searches of electronic devices. Upon release of these revised policies, "the Secretary [of DHS] directed that CRCL assess the impact of these policies, to ensure that civil rights and civil liberties concerns are appropriately addressed and to look for ways in which the new polices might be improved." *Id.* at 1. Among other things, the Impact Assessment recommended that CBP conduct analyses to assess whether certain populations were disproportionately subject to border searches of electronic devices, to share the information with CRCL, and if a disproportionate effect was found, to work with CRCL on developing appropriate oversight mechanisms. *Id.* at 3-4.[1]

12. The DHS Secretary requested that CRCL "look for ways in which the new policies might be improved" and evaluate whether policy changes, such as the development of appropriate oversight mechanisms, were necessary. The 271 pages of spreadsheets and analyses withheld from the March 15, 2019 release reflect the ongoing exchange of

[1] CRCL did not find evidence that the searches were prompted by the ethnicity of travelers. [CRCL Impact Assessment, Border Searches of Electronic Devices 3, https://www.dhs.gov/sites/default/files/publications/crcl-border-search-impact-assessment_01-29-13_1.pdf].

information between CBP and CRCL to allow CRCL to gain information about CBP's policies, with the anticipation of future policy recommendations to agency leadership. These records were created for the specific purpose of evaluating whether changes to policies might be necessary and to make recommendations to agency leadership regarding potential changes to those policies. They were considered by CBP and CRCL to be Law Enforcement Sensitive and For Official Use Only and were treated as such, with their distribution being limited to DHS personnel with an official need to know. The identification of these records as Law Enforcement Sensitive and For Official Use Only has not changed in the time since these records were so marked and provided to DHS.

13. As such, the spreadsheets and analyses were developed in the course of DHS's internal, predecisional deliberations regarding the conduct of border searches of electronic devices and to inform policymakers on whether to make recommendations to departmental decision makers regarding border searches of electronic devices. CRCL is charged with reviewing agency actions and making policy recommendations for consideration by agency leadership. In order to fulfill this function, it is imperative that CBP officials provide comprehensive information to CRCL so that CRCL can evaluate the agency's actions, without the fear by CBP that their frank and candid observations provided in support of that process will be disclosed to the public.

CBP Appropriately Withheld Information From TECS Records To Protect The Privacy Interests of the Traveling Public

14. CBP withheld information from TECS records pursuant to Exemptions (b)(6) and (b)(7)(C) to protect the privacy interests of the subjects of those records. The

information withheld for these reasons includes information that could be used to identify the subject of a particular record. The data CBP withheld from TECS records pursuant to Exemptions (b)(6) and (b)(7)(C), either on their own or taken together as a whole, could lead to the identification of the subject of the record and reveal personal information of the subject of the record.

15. CBP produced two thousand pages of Electronic Media Reports (EMRs), also known as Inspection of Electronic Media (IOEM) records from TECS, CBP's primary law enforcement database. An EMR is created to document every CBP border search of an electronic device. Additional information regarding documentation of border searches of electronic devices is available at https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf.

16. Each time a CBP officer conducts a border search of an electronic device, an EMR is created to document the search. EMRs include multiple standard fields and a narrative description of the border search. EMRs include a great deal of information regarding the traveler which, individually and/or taken together, can lead to identification of the subject of the law enforcement record.

17. While some fields in the EMR and information included in the narrative can reveal a person's identity directly (e.g., name, passport number, date of birth), other pieces of information reveal a person's identity when taken together with the rest of the document. For example, the subject of the record can be identified not only by personally identifiable information contained on the face of the record, but also by non-identifying biographic information (e.g., ethnicity, country of birth, citizenship,

occupation, purpose and/or duration of a trip). When all that information is taken together, it can lead to identification of the subject of the record. Moreover, identification is possible when that information is combined with other information that is publicly available or known to third parties. For example, a media report may contain certain biographic information about an individual identified in the report that could be cross-referenced against information contained in CBP records to reveal additional information about the individual's encounter with CBP.

18. An individual's identity may be revealed not only by cross-referencing information in government records with publicly available information, but also by revealing information to third parties – for example, family members or personal associates – that are privy to personal details about the individual, even if such details are not contained in publicly available sources. For example, a friend, neighbor, or family member may know an individual's ethnicity and occupation and that the individual crossed the border on a certain day and could view disclosed records to gain details about the border inspection.

19. The relative infrequency with which CBP conducts border searches of electronic devices also plays a role. In fiscal year 2017, for example, approximately 0.007 percent of the approximately 397 million arriving international travelers processed by CBP officers had their electronic devices searched (approximately 18,400). As a result, if CBP were to disclose more biographical information regarding individuals subject to device searches, it would be relatively easy for a third party to review searches that meet certain criteria (e.g., the searched occurred on a certain date, involved an individual of a certain ethnicity or country of birth, and the individual had a certain

occupation) and isolate searches of interest from the limited universe of CBP device searches. The information from CBP records could then be correlated against other available information – either publicly known or known to the third party – to identify the subject of the search and tie that person to the CBP record, without his or her authorization or consent. This would reveal not only that the individual was subject to a border search of an electronic device, but also any other unredacted personal details contained in the record (including, for example, whether the individual had a travel companion or whether the individual was cooperative).

20. The risk that disclosure of the information redacted pursuant to Exemptions (b)(6) and (b)(7)(C) from the EMRs will make it possible that the records can be tied to specific people is amplified in light of the volume of records produced in this case. This is especially true with respect to potential identification by individuals who know the subject of the record. As a hypothetical example, a reference to an accountant whose country of origin is Italy whose device was searched on a particular date after a two-week trip to Japan may not appear on its face to reveal the identity of the individual, but there is a substantial likelihood that his friends, neighbors, and clients would recognize the description. In other words, even if *the plaintiffs* could not identify the subject of an EMR based on the challenged fields, the records that were produced are in the public domain (and plaintiffs have expressed the intention to publish all the records produced) and *other members of the public* would be able to identify the subjects of the records based on the information that was withheld pursuant to Exemptions (b)(6) and (b)(7)(C).

21. In processing records under FOIA, CBP works to promote transparency; however CBP must also fulfill its obligation to protect privacy rights. The public interest in specific law enforcement records does not outweigh the privacy interests of members of the public to prevent disclosure of information in specific law enforcement records that could be tied to them. Consequently, exemptions (b)(6) and (b)(7)(C) were applied to prevent the identification of the subjects of the law enforcement records at issue.
22. Due to the privacy interests associated with law enforcement records about individuals, at times CBP makes the determination to fully withhold records regarding inspections of the traveling public unless the individual expressly authorizes release of the record and waives applicable rights against disclosure. As a policy matter, CBP applies the same protections to information regarding aliens that it applies to citizens. Due to the substantial public interest relating to CBP's authority to inspect electronic devices at the border, CBP determined in this case that the release of limited information from these law enforcement records was appropriate under FOIA. However, CBP withheld any information that could be used to identify the subject of the record under exemptions (b)(6) and (b)(7)(C).
23. CBP records detailing border searches of electronic devices are law enforcement records that contain personal details about travelers acquired during the course of border inspections. At times, the privacy interests associated with this information is clear on its face. In other cases, even mundane information – such as the date an individual traveled, the duration and purpose of his or her trip, the presence of co-travelers, the individual's profession, and even the fact that the individual experienced a device search – can implicate substantial privacy interests. Identifying information

about the subject of a border inspection of an electronic device *in law enforcement records and narratives* was withheld pursuant to Exemptions (b)(6) and (b)(7)(C). In the absence of a waiver or other authorization from the subject of the record, disclosure of such information would represent an unwarranted invasion of personal privacy. Notably, this is distinct from records including aggregate or statistical information unconnected with a specific law enforcement inspection on a particular day; CBP did not withhold such information pursuant to Exemptions (b)(6) or (b)(7)(C). Instead, CBP asserted Exemptions (b)(6) and (b)(7)(C) over the challenged information as it appeared in specific law enforcement records. The privacy interest of the subject of the record is heightened in this context. This is especially true given the volume of records produced, which would allow for comparison. If the subject of records was uncovered, there would be a clear basis for comparison. In that context, even the comparative length of one narrative as compared to another could be used to attempt to gauge the nature of the search or the government's findings. And given the nature of border inspections – where every individual is obligated to present themselves and their effects for inspection at the border – this privacy interest is heightened. The data at issue is bulk data; while some inspections revealed items of concern, others did not. This is not a situation in which only records of individuals identified as violating the law were requested. In this context, the balance is tipped more heavily on the privacy interest of the subject of the record.

24. The records that were released contain information that implicates the personal privacy rights of travelers. For example, one of the EMRs challenged by Plaintiff involves a January 28, 2017 inspection of a male traveling inbound into the United States.

CBP001517-18. Per the information that was not withheld, the inspection included a quick cursory search of the individual's electronic device with negative results. CBP001518. However, the released record also indicates that the individual refused to comply with multiple requests from the CBP officers performing the inspection. *Id.* Although the record does not describe any unlawful activity or intimate personal details, CBP recognizes that individuals have a general privacy interest in the nature of their interactions with law enforcement, and disclosure of the individuals' identity risks intruding on such privacy interests. Therefore, information in the record that could be used to identify the subject of a specific record was withheld.

25. As an additional example, another EMR describes a January 29, 2017 inspection of an inbound female traveler who was seeking admission to the United States as a tourist. CBP001585-87. Information in the record that was not withheld indicates that the traveler volunteered information that she requested not be included in her sworn statement, that photos from her phone were displayed during the course of the inspection, that the traveler stated that she had voice recordings on her phone to prove the truth of her statements, and that another woman was somehow involved in the visa process. CBP001586. The released record further indicates that the traveler "knew that she did not obtain the proper employment authorization documents to work legally here in the United States." CBP001586-87. CBP considers the traveler to have a privacy interest in the information reflected in this record and redacted the record with the understanding that disclosure of such information in a manner that would allow for identification of the traveler to the public or to a third party (to include other individuals referenced in the record) would constitute an undue invasion of those privacy interests.

26. The two thousand pages of EMRs that were produced contain information about an individual's private life that could be used to ascertain the identity of the subject of any of these records. Therefore, CBP has withheld certain information that could be used to identify the traveler whose device search is documented with an EMR. Information withheld includes an individual's profession, education, specific descriptions of the devices carried, and details regarding their foreign travel and plans upon entry to the United States. These redactions cannot be examined in isolation, but need to be considered in the context of the record and the information that CBP has not redacted in the record. The information challenged by Plaintiffs cannot be segregated from the other identifying information that is contained in the record that CBP seeks to protect. The information, which CBP has left unredacted in the EMRs, includes the date and time of the search, along with the gender and race of the individual. If someone were to know personal information about an individual, such as the type of information that has been redacted, and date of the person's return from international travel, there is more than a mere possibility that the subject of the record may be identified. For example, if the withheld information were released, it would be easy for a student who knew basic information about his professor, like gender and the approximate date of international travel, to ascertain that the record which references a female professor from Spain with two children who teaches anthropology is his professor at the university he attends. As another example, if a traveler complained to his neighbor that his device had been searched upon his return from an international vacation on a certain date, the neighbor could check the EMRs by date to see if she could find one that seemed to meet the description of her neighbor. If the information CBP withheld pursuant to Exemptions

(b)(6) and (b)(7)(C) were revealed, she could identify her neighbor's record. Based on the information that was left unredacted and other factors, such as the length of the record as compared to others, she may draw conclusions – warranted or unwarranted – about her neighbor or view him in a different light.

27. In the absence of a waiver or authorization, CBP withheld the information at issue. If the subject of a record sought their records in FOIA, personally identifiable information about that individual would not be withheld pursuant to (b)(6) and/or (b)(7)(C). On the other hand, when a third party seeks law enforcement records regarding an individual, in the absence of authorization to disclose from the subject of the record, information that can assist in identifying the subject of the record is appropriately withheld pursuant to (b)(6) and (b)(7)(C). If the information is not connected to a specific law enforcement record or encounter – or if aggregate or statistical information is compiled – the balance would be struck differently.

28. For all the reasons identified above, CBP redacted the fields from spreadsheets produced in this case where those fields contained the same information withheld from the EMRs pursuant to Exemptions (b)(6) and (b)(7)(C) and where that information was taken from the EMRs and presented individually for each specific inspection (i.e., the information was not aggregated).

CBP Withheld Information About Sensitive Law Enforcement Techniques and Procedures Pursuant to Exemption (b)(7)(E)

29. The information CBP withheld pursuant to Exemption (b)(7)(E) would reveal sensitive law enforcement methods, techniques, and procedures, including how CBP conducts risk assessments, CBP's law enforcement priorities, and how CBP determines which

actions to take in the context of specific border inspections, in light of CBP's extensive law enforcement responsibilities.

30. The factors that CBP considers in determining which specific actions to take during an inspection are a method and technique CBP employs. Normally, over one million travelers per day go through U.S. ports of entry.[2] Upon arrival in the United States, individuals are generally required to present themselves to CBP at the port of entry's primary arrival location, often referred to as "primary" or "primary inspection." CBP Officers use the available information and their extensive training and experience to identify situations that warrant additional scrutiny. If the CBP Officer at primary determines that additional scrutiny is appropriate (for example, to address concerns related to admissibility, customs, national security, and/or agricultural laws or other laws enforced or administered by CBP), the traveler may be referred for a continuation of the inspection, often referred to as "secondary" or "secondary inspection." A secondary inspection is a continuation of the border inspection and an officer may refer any traveler to secondary inspection.

31. The sheer volume of people and merchandise passing through the border each day means CBP has a limited amount of time to determine the specific law enforcement actions appropriate for each encounter. TECS is CBP's principal law enforcement and counterterrorism database system used at the border to assist with inspections and determinations regarding admissibility of arriving persons. CBP officers use TECS at the border to document inspections and to identify whether there are any relevant

[2] At present, the number of travelers processed by CBP daily has decreased significantly due to issues related to COVID-19, including travel restrictions. The information in this Declaration regarding typical processing numbers does not reflect or account for the present decrease associated with COVID-19.

"lookouts" in the TECs system to advise officers that additional scrutiny may be warranted. CBP's unified border mission responsibilities are varied and complex, and CBP Officers take a holistic approach that accounts for the totality of the circumstances in order to properly evaluate and assess the people and goods that seek to cross the border. Every aspect of the determination of when to refer a traveler or shipment for additional scrutiny, and what specific actions should be taken during a border inspection reflect the methods, techniques, and procedures that CBP officers are trained to undertake.

32. Disclosure of the information withheld pursuant to (b)(7)(E) would reveal CBP priorities and considerations, thereby enabling wrongdoers to evade the methods, techniques, and procedures that were revealed.

33. Plaintiffs challenge the application of (b)(7)(E) to withhold disclosure of the specific reasons for specific searches on specific dates at specific times. The reason a particular traveler's device was searched is a clear example of a CBP method that would present a danger to border security if it was disclosed. While travelers are generally obligated to present themselves for inspection, only a fraction of a percent have their devices searched, so explaining why CBP takes that specific action, especially by disclosing a high volume of records, clearly discloses CBP priorities and how CBP conducts risk assessments in utilizing its finite resources. Given how relatively infrequently CBP conducts border searches of electronic devices, such disclosure could equip a wrongdoer with the ability to evade such inspections, thereby circumventing the law and permitting the introduction of threats from abroad. As noted in the CBP Directive, which is available at https://www.cbp.gov/sites/default/files/assets/documents/2018-

Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf, there are many reasons for which device searches may occur, which include providing additional information relevant to admissibility under the immigration laws and detection of evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, child pornography, and financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. While there may not be a specific reason for each device searched because generally all travelers are obligated to present themselves and their belongings for inspection, the TECS records include a narrative describing each part of the border inspection, including where relevant and appropriate, the specific reasons a device is searched.

34. Disclosure of specific reasons particular devices were searched would reveal tangible law enforcement information that could be exploited. Particularly considering the volume of records at issue, this information would allow those who seek to circumvent the law to assemble a picture of CBP's law enforcement focus and to identify CBP operations during specific timeframes. Revealing information about the reasons for border searches of electronic devices in a high volume of inspection records would provide a basis for comparison of the handling of different inspections, which would reveal the nature and extent of the government's law enforcement interest in particular situations and allow for comparison based on various factors. This could lead those who seek to circumvent the law to adjust their behavior with the goal of decreasing the likelihood that their device will be searched at the border. Specifically, those who would seek to circumvent the law could gauge how often searches are conducted for particular reasons, which would enable them to obfuscate the purpose of their travel or

assess the likelihood that a traveler with a specific type of background would be subject to search. In addition, public release of the reasons for a search on a specific date and time could reveal to a traveler who knew their device had been searched on a certain date and time, the reason their specific device was searched. This would reveal the nature of law enforcement interest in that traveler, which could reveal information about on-going investigations and inquiries. It could also lead the traveler to take evasive actions to avoid future searches, including for example by asking a co-traveler to carry their devices or engaging in surreptitious deletion of all data resident on devices during an inspection.

35. In addition, disclosure of the reason for a border search of an electronic device can reveal information about CBP targeting efforts, ongoing operations, and lookouts. The release of the sensitive information contained in records pertaining to the reason for a specific search, particularly considering the volume of records at issue, would divulge sensitive details regarding targeting and operations. This would have the unintended and undesirable effect of placing CBP's law enforcement techniques and strategies in the public domain and at the disposal of individuals who could evaluate law enforcement priorities and devise methods to evade detection and apprehension; and, ultimately, this would impair the effectiveness of those law enforcement techniques. Disclosure of information pertaining to targeting and operations could risk law enforcement techniques and procedures by revealing the information CBP considers in conducting law enforcement activities, as well as CBP's priorities when conducting these activities. These records would reveal information about inspectional activities generally, such as the kind of information considered important to the exercise of

officer discretion, and the relative weight given different factors. Information about such "red flags," if unprotected, can enable individuals to thwart efforts to secure the border and enforce customs and immigration laws, thereby undermining homeland security.

36. In addition, some descriptions of the reason for a specific search integrate or reference data belonging to third-party agencies or departments. As a preliminary matter, disclosure of such information threatens efforts to foster open communication across agencies and cohesive law enforcement and national security efforts. Disclosure of the information contained in these records could have far-reaching effects, impairing other agencies' law enforcement operations or their ability to effectively carry out their respective missions. Knowledge of this information would increase the risk of circumvention of laws and regulations, impede effectiveness of law enforcement activities, and endanger agency investigative practices and techniques.

37. The CBP Directive provides for notification (including notification through a tear sheet), with certain enumerated exceptions. By law and policy, when a CBP officer conducts a border search of information on an electronic device, the officer must notify the individual subject to the search of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. However, such notification is not required if it would impair national security, law enforcement, officer safety, or other operational interests.

38. Due to the law and policy governing the circumstances in which CBP can withhold the required notification from the traveler, the failure to notify the traveler tends to indicate

that the traveler's knowledge of the full scope and extent of his or her border inspection would impair national security, law enforcement, officer safety, or other operational interests. In other words, letting someone know that one of those exceptions applies to them would reveal the nature of the government's interest in an individual. This applies when individuals request their own records, and the risk is compounded when a large volume of records is sought. Disclosing whether or not the subject of a search received a notification would also tend to reveal the inspecting officer believed the search implicated a national security, law enforcement, officer safety, or other operational interest that would be impaired if the officer notified the individual. And although the records released in this case do not reveal the identity of the individual, the subject of a search may nonetheless deduce that a record pertains to his or her inspection based on the information that is disclosed, which generally includes the date and time and other details relating to the inspection. If CBP also revealed whether or not the individual was notified of the inspection, a traveler who was not notified that a device search occurred could also infer that CBP withheld the notification because CBP determined it would impair national security, law enforcement, officer safety, or other operational interests. This would tend to disclose the nature of the Government's interest in the individual as CBP generally withholds the notification only in certain circumstances. This may, in turn, lead the individual to take additional steps to conceal harmful or illicit material and frustrate future investigative efforts.

39. Information that, if disclosed, would risk circumvention of the law by revealing CBP techniques, procedures, or guidelines for border searches of electronic, appears in a variety of records. Most prominently, EMRs contain details about the nature of CBP's

law enforcement interest in a particular inspection (to include, when applicable, the reason for the search), the techniques used by CBP to further the agency's investigative interest, and CBP's evaluation of the law enforcement value of information uncovered during the inspection. This information may be reflected in certain fields used by the agency to categorize or code important aspects of the inspection, or it may be reflected in narrative sections that allow for the entry of free text.

40. However, sensitive information associated with CBP's border searches of electronic device is not limited to EMRs. CBP utilizes the information memorialized in EMRs to create other types of records. For example, CBP uses information memorialized in EMRS to generate reports and spreadsheets that include information regarding numerous individual inspections. The incorporation of this data into a new format does not alter the underlying sensitive nature of this law enforcement information. In fact, in certain respects, the aggregation of information regarding many individual searches may increase the degree to which disclosure would impair CBP's law enforcement interests, as the compilation of this information may reveal trends and vulnerabilities in CBP's law enforcement operations. For example, aggregated information can reveal the historic probability that a device search will occur under certain circumstances, or it may reveal the reasons CBP typically initiates device searches. Such information can be used by illicit actors to gauge the likelihood that they will experience a search under certain circumstances and to take steps to avoid scrutiny. For this reason, CBP redacted the same types of information it redacted from EMRs from spreadsheets and reports that contain information about multiple individual border searches.

41. CBP also redacted aggregate statistics from spreadsheets and reports regarding border searches of electronic devices to the extent such statistics tend to disclose CBP's law enforcement techniques, procedures, and guidelines, and disclosure would risk circumvention of the law. For example, disclosure of the relative frequency with which devices are searched at each specific port of entry may reveal the tendencies or frequency of the use of certain inspection techniques, like border searches of electronic devices. Revealing this information poses a risk of circumvention of the law by providing illicit actors the opportunity to identify different practices and techniques employed at different locations and modify their behavior accordingly at a particular port or choose to travel through a specific port. Similarly, revealing aggregate statistics about the nationality of travelers who have devices that are subject to a border search tends to provide insight into non-public sources of information and methodologies used by CBP in performing its law enforcement and border security duties. For example, a high number of individuals of a certain nationality whose devices were searched on days that correspond to a flight from that country that lands at a particular airport may reveal the existence of an ongoing operation at that airport. Disclosing this information poses a risk of circumvention of the law by providing potential adversaries the ability to identify circumstances in which a device search may be more or less likely, or by revealing the capabilities or vulnerabilities of CBP inspection techniques. Additionally, release of this information, without context, may jeopardize the relationship that CBP has with foreign partners based on the relative frequency with which device searches are performed on travelers of any particular nationality compared to travelers of another nationality. This could have a negative impact on CBP's cooperative activities and

information sharing with that country, which CBP relies on to assist in identifying illicit actors or threats to border security.

CBP Withheld Information From Complaint Records Pursuant to Exemptions (b)(6), (b)(7)(C), and (b)(7)(E)

42. Sensitive information from CBP law enforcement records, including EMRs, is also used by CBP personnel responsible for reviewing, evaluating, and responding to complaints submitted by members of the traveling public. At times, this information is incorporated directly into the internal record system used by CBP to process complaints in order to provide background information and context to CBP personnel tasked with researching, resolving, and responding to complaints. Thus, CBP complaint records include both new information – which is reviewed and compiled, among other reasons, for law enforcement purposes to identify potential criminal or administrative misconduct and identify potential waste, fraud, or abuse – and information obtained from existing CBP records that were compiled for other law enforcement purposes (e.g., EMRs).

43. The incorporation of information from CBP law enforcement records (e.g., EMRs) into CBP's complaint system does not change the sensitive nature of the information. In certain respects, it increases the need to prevent disclosure given the fact that it ties the complaint to the law enforcement activity memorialized in the other record. If that information were to be disclosed as part of the complaint record, it would provide the individual who submitted the complaint insight into the nature of the law enforcement records maintained by CBP relating to the encounter. The fact that CBP anonymized the complaint records produced in this case would not prevent the individual who

submitted the complaint from making the association, as the complainant can still identify his or her own complaint, even if third parties cannot.

44. The disclosure of additional law enforcement information contained within CBP complaint records would also constitute an unwarranted invasion of personal privacy. An individual who submits a complaint to CBP has a privacy interest not only in the substance of the complaint, but also in information compiled by CBP in processing the complaint, particularly information drawn from CBP law enforcement records about the individual. To prevent the disclosure of information that would cause an unwarranted invasion of personal privacy, CBP redacted information from the complaint records that could lead to the identification of the subject of the complaint. Nevertheless, the complaint records produced by CBP in this case contain some details about the individual and their encounter with CBP. In many instances, CBP disclosed certain types of information in traveler complaint records that was redacted from CBP law enforcement records such as EMRs. The reason relatively more information was disclosed in complaint records is twofold. First, in the case of traveler complaints, the individual has volunteered the information contained within the complaint itself, whereas information contained in law enforcement records is generally obtained during the course of a border inspection. Second, EMRs are produced for every border search of an electronic device conducted by CBP, whereas an individual submits a complaint in just a small fraction of cases. As a result, most device searches do not have a corresponding complaint record, which decreases the risk that the subject of a complaint record can be identified by a third party that merely knows that CBP conducted a device search of a particular individual in a certain day. Therefore, the risk

of inadvertently revealing the identity of the individual is decreased in some respects in the case of complaint records.

45. Because many complaint records have additional non-identifying information about the subject of the search, the combination of information from the traveler complaint with law enforcement information incorporated into the complaint record increases the risk that disclosure will lead to the identification of the complainant, either based on the information contained in the record or combined with other available information. It also increases the potential privacy implications associated with disclosure of the individual's identity, as it would reveal not only that the individual submitted a complaint, but also that the information is the subject of a law enforcement record.

46. It is my understanding that Plaintiff has generally challenged the (b)(6), (b)(7)(C), and (b)(7)(E) exemptions applied to the complaint records produced in this case and that Plaintiff specifically identifies the redaction of the second and third pages of the complaint record that begins at CBP005274. Dkt. 48, at 37. The particular complaint record cited in Plaintiff's brief includes the complainant's submission to CBP and CBP's response, as well as internal communications and notes that CBP personnel added to the record during processing of the complaint. CBP005274-78. The types of information that CBP withheld from the complaints, including this records, are discussed in my January 30, 2020 Declaration and pages 17-20 of the accompanying *Vaughn* index.

47. Notwithstanding the redactions made by CBP, the released record reveals the substance of the complaint and CBP's response, including certain personal details communicated by the complainant to CBP, including his or her country of origin (Canada), certain

travel details ("I was traveling on the scheduled 11:30am BoltBus to arrive in Seattle at 3:30pm"), the traveler's participation in certain trusted traveler programs (NEXUS and Global Entry), and details about the inspection ("CBP officers went through my mobile phone and laptop"; "[d]rug detection dogs were brought to patrol around me three times"; "[t]wo FBI agents also were called in to interview me near the end").

48. The redaction referenced by Plaintiff – the second and third pages of the record beginning at CBP005274 – consists of information extracted from a CBP law enforcement record that was incorporated directly into the complaint record and was consulted by CBP personnel during the processing of the complaint record in question, and it was redacted for the reasons described above, the reasons contained in my January 30, 2020 Declaration in this case, and the reasons described in CBP's *Vaughn* index. As set forth in the *Vaugh* index, the information withheld under exemptions (b)(6) and (b)(7)(C) includes, among others things, "results of queries of law enforcement systems" and "subject-specific law enforcement information and outcomes." CBP *Vaughn* at 17-18. The redaction at issue falls within these categories. The redaction also includes a variety of other types of information that could, whether standing alone or combined with other available information, identify the subject of the record, his or her associates, or CBP personnel, including: names, unique record numbers, travel document numbers, email addresses, and travel itineraries. *See id.* CBP also withheld information from the record under exemption (b)(7)(E) including, among others things, "the reason for the search," "information regarding coordination with specialized units and law enforcement partners," and "descriptions of the law enforcement records consulted or created when investigating complaints." *Id.* at 19.

Disclosure of the information redacted from this document would constitute an unwarranted invasion of personal privacy by identifying the subject of a CBP law enforcement record and would disclose law enforcement techniques, procedures, and guidelines and thereby risk circumvention of the law. Notwithstanding the redactions made for these purposes, CBP released the information that was reasonably segregable from the exempt information, including a substantial amount of detail about this complaint and CBP's response.

CBP Withheld Information From Internal CBP Communications and Memoranda Pursuant to Exemptions (b)(6), (b)(7)(C), and (b)(7)(E)

49. It is my understanding that Plaintiff also challenges the exemptions applied to internal CBP communications and memoranda relating to border searches of electronic devices. In particular, Plaintiff references a January 2009 "muster" relating to CBP policies on device searches. CBP Mar. 15, 2019 Release, at 43-44. It is my understanding that a "muster" is a type of memorandum used by CBP's Office of Field Operations to communicate important information to CBP Officers, who are the federal law enforcement officers at U.S. ports of entry responsible for enforcing customs, immigration, and other laws enforced or administered by CBP.
50. Other than two redactions under exemptions (b)(6) and (b)(7)(C) to withhold the name and/or contact information of a CBP employee, the remaining redactions were made under (b)(7)(E). As set forth in the CBP *Vaughn* index, information redacted from internal policies and memoranda under exemption (b)(7)(E) includes "information that would reveal the scope and focus of inspections techniques, factors relevant to criteria

for utilizing particular inspections methods, . . . focus or scope of device searches and other inspection techniques, . . . [and] information regarding the specific technical capabilities utilized during certain type of inspections . . . ." CBP *Vaughn* at 2. These descriptions apply to the redactions from the January 2009 muster. The information CBP withheld from this record under (b)(7)(E) describes specific procedures and guidelines for border searches of electronic devices and techniques utilized to conduct such searches, including factors to be considered by CBP Officers when determining whether to utilize specific capabilities when conducting a device search at the border, which, if disclosed, would reveal the scope and focus of CBP device searches under particular circumstances. Disclosure of such information in this record or other internal CBP policies and memoranda would risk circumvention of the law by permitting illicit actors to determine the scope of CBP's technical capabilities, gauge the relatively likelihood that they would be subject to a device inspection under certain circumstances, and if subject to inspection, infer the reason for or focus of CBP's law enforcement interest. Such information could then be used to develop countermeasures, avoid detection, and frustrate CBP's ability to detect illicit activity and enforce the law. CBP also redacted similar information – including factors to be considered by CBP Officers when determining whether to utilize specific capabilities when conducting a device search and information regarding the specific focus of CBP device searches under particular circumstances – from the "Pilot Program" Powerpoint presentation produced to Plaintiff in this case. CBP000212-34; CBP *Vaughn* at 11-13. Like the internal policies and memoranda discussed above, CBP used the Powerpoint presentation to communicate policies, procedures, and technical capabilities regarding

device searches to CBP Officers. The presentation also addresses specific techniques utilized by CBP to conduct device searches and circumstances in which such techniques may be more likely to be utilized. The fact that CBP communicated this information to officers in presentation form does not alter the underlying sensitivity of the information or the fact that its disclosure could lead to circumvention of the law. Disclosure of such information in this record would risk circumvention of the law by permitting illicit actors to determine the scope of CBP's technical capabilities, gauge the relatively likelihood that they would be subject to a device inspection under certain circumstances, and if subject to inspection, infer the reason for or focus of CBP's law enforcement interest. Such information could then be used to develop countermeasures, avoid detection, and frustrate CBP's ability to detect illicit activity and enforce the law.

51. It is my understanding that Plaintiff also challenges CBP's redaction of information in "internal communications and correspondence with CRCL." Dkt. No. 48, at 25 & n.37 (citing CBP005115, CBP005117, Mar. 15, 2019 Release, at 2-3, 3-37, 42-51, 55-61, Mar. 22, 2019 Release, at 1-17, 26-28, 70-79, Aug. 2, 2019 Release, at 1-84). The records cited by Plaintiff consist of materials created by or provided to CRCL in connection to CRCL's review of CBP activities, as described in CBP's *Vaughn* index. CBP *Vaughn* 23-27. In the course of reviewing CBP activities, CRCL requested and CBP provided records relating to the manner in which CBP utilizes border searches of electronic devices in the exercise of its law enforcement duties. This information included CBP policies and procedures relating to device searches, as well as CBP law enforcement records memorializing device searches and summaries thereof. In

addition, CBP conducted its own internal analyses of the manner in which the agency utilized border searches of electronic devices, which CBP shared with CRCL. CRCL and CBP also exchanged information relating to specific inspections in which CRCL received complaints from the public relating to border searches of electronic devices. The information generally described by Plaintiff's as "internal communications and correspondence with CRCL" encompasses all of these types of records, the vast majority of which are not simply correspondence between CBP and CRCL, but also include background material, policies, law enforcement records, and analyses provided by CBP to CRCL to facilitate its review.

52. Because these records document the manner in which CBP exercises its law enforcement authorities, they contain information regarding specific law enforcement techniques, procedures, and guidelines relating to border searches of electronic devices. The fact that CBP provided this information to CRCL does not alter the underlying sensitivities associated with this law enforcement information and does not obviate the need to maintain its confidentiality in order to prevent circumvention of the law. For this reason, CBP redacted similar types of information from the records exchanged with CRCL that it redacted from other law enforcement records, such as EMRs and internal CBP policies and memoranda relating to border searches of electronic devices.

53. It is my understanding that Plaintiff references three records in particular in its challenge to CBP's (b)(7)(E) redactions in the records relating to CRCL's review, specifically: (1) CBP Internal Affairs Report: Border Search of Electronic Devices and Documents, CBP's Mar. 15, 2019 release (p. 37); (2) Electronic Device Inspection: A Follow-Up Study to CRCL, CBP's Mar. 22, 2019 release (pp. 1-17); and (3) CBP

Comment on CRCL Impact Assessment for Border Searches of Electronic Devices, CBP's Mar. 22, 2019 release (pp. 70-79). In order to engage in a full and open dialogue with CRCL, CBP provided CRCL with sensitive law enforcement information. Thus, each of these records contain descriptions and analyses of the techniques, procedures, and guidelines used by CBP to conduct border searches of electronic devices. For example, the portion of the "Findings" withheld from the record entitled CBP Internal Affairs Report: Border Search of Electronic Devices and Documents (CBP's Mar. 15, 2019 release, p. 37) contains specific details of CBP's techniques, guidelines, and procedures for conducting border searches of electronic devices. The other two documents cited by Plaintiff – Electronic Device Inspection: A Follow-Up Study to CRCL (CBP's Mar. 22, 2019 release, pp. 1-17) and CBP Comment on CRCL Impact Assessment for Border Searches of Electronic Devices (CBP's Mar. 22, 2019 release (pp. 70-79) – consist, in part, of statistical analyses of the circumstances in which CBP conducts border searches of electronic devices. In order to conduct the statistical analyses, CBP identified a subset of device searches that met certain law enforcement criteria. The disclosure of the information withheld by CBP would reveal law enforcement techniques and procedures used by CBP to identify individuals for inspection and reveal the circumstances in which an individual may be more likely to experience an inspection of his or her electronic device.

54. As described in CBP's *Vaughn* index, the information redacted from these records under (b)(7)(E) includes, among other things, "information that would reveal the scope and focus of inspections techniques, . . . information regarding law enforcement alerts or lookouts, descriptions of the tendencies or the frequency with which certain

inspection techniques occur at various ports or locations, analysis of the frequency with which certain types of law enforcement encounters occur at various locations or under certain conditions, . . . descriptions of factors, criteria or methods considered when deciding whether to utilize certain inspection methods, recordkeeping requirements that reveal the reason, scope of focus of certain inspection techniques, . . . and descriptions of the handling, maintenance and storage of law enforcement or national security information obtained from a border inspection." CBP *Vaughn* at 26-27. CBP also redacted from the records "[i]nformation that, when aggregated, could reveal inspection trends that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law," including port locations, biographical information regarding subjects of inspection, and reason for search. Disclosure of such information would risk circumvention of the law by giving illicit actors insight into the circumstances in which CBP tends to employ certain inspection techniques – such as border searches of electronic devices – and allow those individuals to modify their behavior in order to decrease the likelihood that they will be subject to such techniques or to employ countermeasures if they conclude they will be at higher risk of coming under law enforcement scrutiny.

55. Plaintiff's reasoning that revealing information would not lead to circumvention of the law also ignores the fact that often travelers do not travel alone. Evasion techniques could include passing off devices to co-travelers that they believe, based on the information revealed, may be less likely to have their devices searched.

SEGREGABILITY

56. CBP has accounted for all responsive records pursuant to the request. Where appropriate, CBP asserted FOIA exemptions in the responsive records. All information withheld is exempt from disclosure pursuant to a FOIA exemption or is not reasonably segregable because it is so intertwined with protected material that segregation is not possible or its release would reveal the underlying protected material. CBP personnel have reviewed the documents determined to be responsive, line-by-line, to identify information exempt from disclosure or for which a discretionary waiver of exemption could apply, and all reasonably segregable portions of the relevant records have been released to the Plaintiff in this matter. In my determination, any further release of the exempted materials could reasonably lead to the identification of individuals or other items that are properly protected by the exemptions asserted.

I declare under a penalty of perjury that the information provided is true and correct to the best of my information, knowledge, and belief.

Signed this 11th day of June 2020.

Patrick Howard

Patrick A. Howard
Branch Chief
FOIA Division
Privacy and Diversity Office
Office of the Commissioner
U.S. Customs and Border Protection
U.S. Department of Homeland Security