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

Defendants' Motion for Summary Judgment

Ex. C

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 and the attached *Vaughn* Index is to provide additional information as to why certain information was withheld from public disclosure pursuant to 5 U.S.C. §§ 552 (b)(3), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E) and 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 their 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, 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 referrals from TSA, all of which were partially released. In addition, CBP processed 1,285 pages of referrals from DHS.

JUSTIFICATION FOR WITHHOLDING INFORMATION UNDER FOIA

Exemption (b)(3)

7. Section 552(b)(3) of Title 5 of the U.S. Code exempts from disclosure certain records or information that are "specifically exempted from disclosure by statute."

8. As explained in greater detail in the attached Index, in this case, two pages of records regarding a specific traveler were withheld in full pursuant to Exemption (b)(3) based on the application of the limitations on disclosure in 8 U.S.C. § 1367. The record in question contained information regarding an alien who is allegedly a beneficiary of an application for relief under 8 U.S.C. § 1101(a)(15)(T), 15(U), or (51) or 8 U.S.C. § 1229b(b)(2).

Exemption (b)(5)

9. Section 552(b)(5) of Title 5 of the U.S. Code exempts from disclosure "inter-agency or intra-agency memorandums or letters that would not be available by law to a party other than an agency in litigation with the agency, provided that the deliberative process privilege shall not apply to records created 25 years or more before the date on which the records were requested."

10. As explained in greater detail in the attached Index, in this case, Exemption (b)(5) has been applied with respect to internal inter-agency and intra-agency memoranda, communications, correspondence, and reports created less than 25 years prior to the record request in this case. Within those records, information protected from disclosure by the deliberative process privilege was withheld.

11. In this case, certain documents and portions of documents were withheld under exemption (b)(5) based upon the deliberative process privilege that is incorporated into exemption (b)(5). The general purpose of this privilege is to

prevent injury to the quality of agency decisions. Specifically, three policy purposes have been consistently held to constitute the bases for this privilege: (1) to encourage open, frank discussions on matters of policy between subordinates and superiors; (2) to protect against premature disclosure of proposed policies before they are finally adopted; and (3) to protect against public confusion that might result from the disclosure of reasons and rationales that were not in fact ultimately the grounds for an agency's action. Logically flowing from the foregoing policy considerations is the privilege's protection of the decision-making process of government agencies. In concept, the privilege protects not merely documents, but also the integrity of the deliberative process itself where the exposure of that process would result in harm. One of the most important factors CBP considers in applying Exemption 5 is the role that the document plays in the process of agency deliberations.

12. As explained in greater detail in the attached Index, in this case, CBP applied the (b)(5) Exemption to documents and information that were deliberative in nature and compiled in advance of a final agency decision. The information withheld under the (b)(5) Exemption includes documents prepared to inform agency decisions; documents that reflect analysis undertaken to support recommendations to agency leadership; draft documents reflecting proposed agency activities; communications among agency leadership and policy advisers containing recommendations, evaluation or comments regarding proposed agency actions,; and documents reflecting agency deliberations and consideration of policy recommendations. Release of the information withheld

in this case would reveal agency deliberations and negatively impact the decision-making process.

Exemption (b)(6)

13. Section 552(b)(6) of Title 5 of the U.S. Code exempts from disclosure certain records and information "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." This exemption requires balancing the public's right to disclosure against an individual's right to privacy. In this case, the information CBP withheld is exempted from disclosure because the privacy interests in that information outweigh the public interest in its disclosure.

14. As explained in greater detail in the attached Index, in this case, Exemption (b)(6) has been applied with respect to internal CBP policies and memoranda; inspection records that document specific border inspections of electronic devices, including electronic media reports (EMRs); certain information contained within complaint records and responses and responses to DHS TRIP redress requests; internal audit and review documentation; and an internal presentation.

15. Within these records, Exemption (b)(6) has been applied to protect the personal privacy interests of CBP personnel, travelers whom CBP personnel have encountered at ports of entry, and other members of the public; exemption (b)(6) has been applied to: (1) personally identifiable information of government employees, including information that could identify CBP personnel involved in law enforcement functions; (2) information regarding the

subjects of records; and (3) information regarding individuals mentioned in records (e.g., co-travelers or other individuals identified or mentioned by the subject of a record).

16. CBP withheld, pursuant to Exemption (b)(6), biographic and biometric personally identifiable information related to specific employees, such as names, signatures, photographs or images, contact information, telephone numbers, email addresses, physical addresses, physical descriptions, badge numbers, and identification numbers and other unique identifiers that could identify CBP or other government personnel involved in a border inspection, compiling records, processing complaints, or compiling information. Release of this information would constitute a clearly unwarranted invasion of privacy. Government employees, including CBP law enforcement officers, have a protectable privacy interest in their identities that would be threatened by disclosure. Similarly, government employees have a protectable privacy interest in their contact information that would also be threatened by disclosure. Release of this information would not shed light on the actions of CBP and there is no public interest in the disclosure of this information. Accordingly, the individual's right to privacy outweighs whatever public interest, if any, might exist in knowing the information.

17. Pursuant to Exemption (b)(6), CBP withheld personally identifiable information regarding members of the public that, if released, could impair the personal privacy interests of those members of the public. Federal officials handling personal information may not disclose personal information to a third party,

except in accordance with the Privacy Act and consistent with the routine uses identified in the System of Records Notices published in connection to each system of records at issue. In this case, Knight First Amendment Institute at Columbia University explicitly requested records regarding third parties, specifically, travelers whose devices were inspected at the border, and information about other third parties that were included in related documents. The Plaintiff has not submitted authorization (e.g., a Privacy Act Waiver) from any individuals permitting the disclosure of information to the Plaintiff; therefore, those third parties maintain privacy interests in their own information, and disclosure is only authorized in accordance with the requirements of the Privacy Act. Consequently, as a third party requestor who has not submitted authorization, the Plaintiff has not received the same access that the subject of records (or those the subjects have authorized) would receive.

18. CBP withheld, pursuant to Exemption (b)(6), personally identifiable information regarding members of the public that were the subjects of agency records. For example, this includes information that, taken in isolation or combined with other information, could reveal the identity of individuals who submitted complaints regarding CBP inspections or practices, and individuals whose devices were inspected by CBP at the border. Public disclosure of information that would identify the subject of a CBP record would be an invasion of personal privacy. Individuals have a privacy interest in protecting their identities, and in choosing whether to disclose the details of an encounter with a law enforcement agency. Identifying individuals who were the subject of

specific agency records or whose electronic devices were searched at the border would constitute a clearly unwarranted invasion of personal privacy. Consequently, any information that could be used to identify the subject of a relevant agency record has been withheld pursuant to Exemption (b)(6). The records at issue also include personal information regarding members of the public and their practices, such as information the individual supplied to CBP or that was identified during system queries. Information that was withheld pursuant to Exemption (b)(6) includes: names, dates of birth, countries of birth, citizenship, travel document numbers, visa category, citizenship/immigration status, identification numbers, document issue/expiration dates, device information, physical addresses, physical description, height/weight, telephone numbers, email addresses, usernames and social media handles, vehicle identifiers and characteristics, unique record numbers, serial numbers, travel history, travel plans, information regarding the purpose of international travel and actions taken during international travel, carrier and flight number, personal history, familial relationships, educational history, occupation information and professional history, place of residence, intimate personal details, criminal history, description of law enforcement information regarding a specific individual, results of system queries, medical information, financial information, political views, asylum information, and descriptions of subject-specific law enforcement information or outcomes.

19. CBP also withheld, pursuant to Exemption (b)(6), personally identifiable information regarding members of the public who were mentioned in agency

records but are not the subject of the record. For example, this includes individuals who are mentioned by the subject of the record or otherwise associated with the subject of the record. Individuals have a privacy interest in protecting their identities, and in choosing whether to disclose their association with an individual who is the subject of a particular government record. This is particularly true where information is supplied by a third party member of the public, and may or may not be accurate. Consequently, any information regarding members of the public who were mentioned in a record but not the subject of the record has been withheld pursuant to Exemption (b)(6). The same categories of information that were withheld with respect to subjects of records was withheld with respect to members of the public who were mentioned in records but are not the subject of the record.

20. Third party individuals have a protectable privacy interest in their identities and personally identifiable information that would be threatened by disclosure. Accordingly, the individual's right to privacy outweighs whatever public interest, if any, might exist in knowing the information. On that basis, CBP withheld information pursuant to Exemption (b)(6).

Exemption (b)(7)(C)

21. Section 552(b)(7) of Title 5 of the U.S. Code exempts from disclosure certain records or information that are "compiled for law enforcement purposes." The records at issue in this case were compiled for law enforcement purposes in that

the information is created and used by CBP in its law enforcement mission to secure the border of the United States.

22. Section 552(b)(7)(c) of Title 5 of the U.S. Code exempts from disclosure law enforcement records or information that "could reasonably be expected to constitute an unwarranted invasion of personal privacy." This exemption extends to CBP as a law enforcement agency. Exemption (b)(7)(C) is designed to protect, among other things, law enforcement personnel from harassment and annoyance in the conduct of their official duties and in their private lives, which could conceivably result from the public disclosure of their identity. The privacy interest in the identity of an individual in the redacted document outweighs any public interest in disclosure of that information.

23. The records provided in response to Plaintiff's request were compiled for law enforcement purposes in that the information contained within these records is created and used by CBP in its mission to secure the borders of the United States. Government employees have a protectable privacy interest in their identities that would be compromised by the release of this information. Similarly, the third party individuals whose personally identifiable information and other identifying details appear in the records have a protectable privacy interest in their identities that would be compromised by the release of this information. In addition, identifying the specific individuals whose information was withheld would not serve a public purpose. Accordingly, the individual's right to privacy outweighs whatever public interest, if any, might exist in knowing this information.

24. Exemption (b)(7)(C) has been applied to the same categories of records and types of information to which Exemption (b)(6) was applied, when the information was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy. As explained in greater detail in the attached Index, in this case, Exemption (b)(7)(C) has been applied with respect to internal CBP policies and memoranda; inspection records that document specific border inspections of electronic devices, including electronic media reports (EMRs); certain information contained within complaint records and responses and responses to DHS TRIP redress requests; internal audit and review documentation; and an internal presentation.
25. Within these records, Exemption (b)(7)(C) has been applied to protect the personal privacy interests of CBP personnel, travelers whom CBP personnel have encountered at ports of entry, and other members of the public; exemption (b)(7)(C) has been applied to: (1) personally identifiable information of government employees, including information that could identify CBP personnel involved in law enforcement functions; (2) information regarding the subjects of records; and (3) information regarding individuals mentioned in records (e.g., co-travelers or other individuals identified or mentioned by the subject of a record).
26. Pursuant to Exemption (b)(7)(C), CBP has withheld personal information contained in documents maintained and compiled for law enforcement purposes, including law enforcement policies, memoranda and a presentation

materials; certain information compiled internally during consideration of incoming complaints, queries, or redress requests; and information prepared in connection to internal audits and reviews of law enforcement activities, when that information would constitute a clearly unwarranted invasion of personal privacy.

27. Pursuant to Exemption (b)(7)(C), CBP has also withheld personal information in documents maintained in TECS, which contains enforcement, inspection, and intelligence records which are relevant to the customs, immigration, agriculture, national security, border security, anti-terrorism and law enforcement missions of CBP and numerous other Federal agencies that it supports. TECS is one of the primary tools that CBP law enforcement officers, and other personnel with authorized access, regularly use, in order to effectively and efficiently enforce all applicable laws, particularly as it relates to travelers and trade crossing the border into or out of the United States. CBP has also redacted certain personal information taken from TECS records and incorporated into other documents as well as other related documents compiled by CBP. The records at issue were compiled for law enforcement purposes in that the information is collected and used by CBP in its mission to secure the border of the United States.

28. TECS, which is principally owned and managed by CBP, is an overarching law enforcement information collection, analysis, and sharing environment that securely links telecommunications devices and personal computers to a central system and database. This environment is comprised of several modules designed to collect, maintain, and vet data as well as conduct analysis, risk

assessments, and information sharing. TECS contains temporary and permanent enforcement, inspection, and intelligence records relevant to the law enforcement mission of CBP and numerous other federal agencies that it supports. TECS is CBP's principal law enforcement and anti-terrorism data base system. TECS is described in further detail in the Federal Register at 73 Fed. Reg. 77778 (Dec. 19, 2008).

Exemption (b)(7)(E)

29. Section 552(b)(7) of Title 5 of the U.S. Code exempts from disclosure certain records or information that are "compiled for law enforcement purposes." The records at issue in this case were compiled for law enforcement purposes in that the information is created and used by CBP in its law enforcement mission to secure the border of the United States.

30. Section 552(b)(7)(E) of Title 5 of the U.S. Code exempts from disclosure law enforcement records or information that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law."

31. The effectiveness of CBP's mission is dependent to a large extent on the use of sensitive investigative techniques and methods that are not known to the general public. These law enforcement techniques and procedures are critical tools used by CBP officers to efficiently and effectively carry out CBP's mission to secure the border and to prevent threats, including terrorists, their weapons, and other dangerous items, from entering the United States, and to enforce customs,

immigration, agriculture and other federal laws at the border. The disclosure of these techniques and methods would seriously compromise CBP's ability to perform its law enforcement mission at the border.

32. As explained in greater detail in the attached Index, in this case, Exemption (b)(7)(E) has been applied with respect to internal CBP policies and memoranda; inspection records that document specific border inspections of electronic devices, including electronic media reports (EMRs); certain information contained within complaint records and responses and responses to DHS TRIP redress requests; internal audit and review documentation; and an internal presentation.

33. Within those records, Exemption (b)(7)(E) has been applied to (1) information that would reveal the subjects of specific law enforcement interest; (2) information regarding specific law enforcement techniques and operational vulnerabilities; (3) information that, in the aggregate, reveals trends and/or specific law enforcement capabilities and techniques employed in particular operational locations, which can reveal the likelihood of CBP utilizing certain inspection techniques in specific operational locations; and (4) computer codes and other information that can expose CBP computer systems to a risk of unauthorized access or navigation.

34. CBP withheld, pursuant to Exemption (b)(7)(E) information that would reveal the subjects of specific law enforcement interest. This includes the application of Exemption (b)(7)(E) to TECS and other records containing remarks and analysis specific to particular individuals. The records at issue here, among

other things, contain information regarding border inspections; the identification of law enforcement agencies and officers involved, contact information, and respective roles; and actions to be taken by law enforcement officers. The release of this information would have the unintended and undesirable effect of placing these law enforcement techniques and strategies in the public domain, in the possession of the specific individuals whose records are at issue, and at the disposal of other similarly situated individuals; educating them as to the investigative techniques used and thereby assisting them to devise methods to evade detection and apprehension; and, ultimately, impairing the effectiveness of those law enforcement techniques.

35. CBP withheld, pursuant to Exemption (b)(7)(E), information regarding specific law enforcement techniques and operational vulnerabilities. This includes information regarding why a particular law enforcement action (including the border search of an electronic device) was undertaken in any specific case. In addition, the records at issue reveal certain interagency techniques through the integration or referencing of 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. Because of the interconnectivity between CBP's law enforcement databases and those of other agencies, disclosure of the information contained in the database 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, compromise the electronic records system, facilitate improper access to sensitive investigatory and other law enforcement records, impede effectiveness of law enforcement activities, and endanger agency investigative practices and techniques.

36. In addition to information that, in any particular instance, could reveal the nature of CBP's law enforcement interest or concern, pursuant to Exemption (b)(7)(E), CBP also withheld information that would reveal law enforcement techniques, abilities, and procedures when aggregated. For example, certain information, in the aggregate, reveals trends and/or specific law enforcement capabilities and techniques employed in particular operational locations, which can reveal the likelihood of CBP utilizing certain inspection techniques in specific operational locations. This is especially true given the broad nature of the Plaintiff's request and the sheer volume of law enforcement records at issue. Moreover, the TECS records include date stamps, locations where specific law enforcement actions took place, internal IP addresses, contact information and communication methods, instructions on handling inspections of travelers, and similar information that reveals the procedures and techniques used by law enforcement. While some of this data may appear innocuous taken in isolation, such information can place investigative activities in a precise context, pinpoint key players and events, identify critical tools and resources, and reveal the extent and shortfalls of law enforcement's knowledge of criminal or terrorist endeavors and/or immigration violations. Moreover, such information creates a

basis for comparison of the handling of different inspections, which could reveal the nature and extent of the government's law enforcement interest in particular situations. Because this information can be used to clarify or predict a CBP officer's behavior in specific circumstances, the risk of circumvention of enforcement efforts or harm to officers or informants is significant.

37. In addition, the TECS records include information that would reveal the capabilities of TECS, the release of which would impede CBP's law enforcement mission by alerting individuals to how CBP conducts searches of its systems and any limitations. Although a few factors used by CBP officers to conduct border inspections are in the public domain in court opinions or other contexts, the TECS format itself reveals more about the techniques that CBP officers use to conduct border inspections and assess risk than the information that can be gleaned from publically available information. Because the data fields for entering remarks and analysis in TECS are of limited capacity, an officer creating a TECS entry must prioritize the information he or she believes most essential for another officer's decision about when and how to conduct an inspection. Thus, disclosure of the remarks in TECS would reveal not only information unique to those particular inspections, but also 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, could enable individuals to thwart efforts to secure the border and enforce immigration and customs laws. Moreover, information entered into TECS

limited data fields must necessarily be abbreviated. Disclosure of this shorthand communication would serve no legitimate public interest, as its meaning would be irretrievably distorted once taken from the tightly-controlled context in which it is created, interpreted, and shared solely by and between law enforcement personnel.

38. CBP withheld, pursuant to Exemption (b)(7)(E), computer codes and other information that can expose CBP computer systems to a risk of unauthorized access or navigation. Protecting and maintaining the integrity of CBP computer systems is imperative to CBP's ability to effectively and efficiently meet its mission to prevent terrorists, their weapons, and other dangerous items from entering the United States. While DHS/CBP, through its System of Records Notice and Privacy Impact Assessment for its systems, including TECS, have taken considerable efforts to provide the public detailed information regarding CBP systems, without compromising the integrity of the systems, as a critical law enforcement tool employed by CBP to enhance border security, it is imperative that CBP protect TECS and other systems against any potential risk of threat or compromise to ensure CBP is able to effectively carry out its law enforcement mission. Consequently, Exemption (b)(7)(E) has been applied to codes used within CBP law enforcement systems, including TECS, and specific information regarding how to navigate and use CBP law enforcement systems, because this information may enable an individual knowledgeable in computer systems to improperly access the system, facilitate navigation or movement through the system, allow manipulation or deletion of data, and interfere with

enforcement proceedings. Specifically, the computer codes at issue facilitate access to, and navigation through, CBP law enforcement systems. Individuals who know the meaning of the codes would have sufficient law enforcement information regarding how CBP conducts its law enforcement operations, which would permit individuals to alter their patterns of conduct, adopt new methods of operation, relocate, change associations, and effectuate other countermeasures, thus corrupting the integrity of ongoing investigations. Public dissemination of these access codes would reveal the technical capabilities of the system and could permit unauthorized users to manipulate records to avoid recognition, detection and apprehension. It would also arm unauthorized users with the ability to corrupt the integrity of the data contained therein through the alteration/manipulation of such data. In addition, if the system were to be hacked, it would permit the intruder to potentially manipulate the way certain records are created and maintained, which could put at risk ongoing investigations and border security operations. Protecting and maintaining the integrity of TECS is imperative in assisting CBP to meet its mission.

39. Disclosure of the information withheld pursuant to Exemption (b)(7)(E) would reveal techniques used by law enforcement to identify violators and other persons of concern to law enforcement, which would allow wrongdoers to evade detection by law enforcement, thereby circumventing the law and potentially resulting in alteration, loss, damage or destruction of data contained in CBP's computer system.

SEGREGABILITY

40. Plaintiff has been provided with all responsive records pursuant to its request. Where appropriate, CBP asserted FOIA exemptions in the released 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 have revealed 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 the 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 30th day of January 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

Attachment

Document Type	Bates Numbers or Release Dates	Disposition	Description and Applicable Exemptions
Internal CBP Policies and Memoranda	000033-36 000054-56 March 15, 2019 release (pp. 33-35, 42-54, 57-61) Aug. 2, 2019 release (pp. 68-70)	Released with partial redaction	Internal policies and memoranda compiled for law enforcement purposes to communicate information and agency policy to law enforcement personnel: (b)(5) • Detail of routing forms used to track the internal review by agency personnel of proposed agency policies, memoranda, and correspondence, the disclosure of which would reveal deliberative, pre-decisional information regarding the agency decision-making process. Redacted information includes: information regarding which offices or personnel were or were not consulted, markings denoting clearance of or objection to a draft proposal, and internal categorization of the draft proposal. (b)(6) • Information that could identify CBP personnel involved in law enforcement functions, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, telephone numbers, signatures, and email addresses. (b)(7)(C) • The information listed above was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy.

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 26 of 58

			(b)(7)(E) • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: information that would reveal scope and focus of inspection techniques, factors relevant to or criteria for utilizing particular inspection methods, descriptions of the law enforcement records consulted or created as part of certain inspections, descriptions of the circumstances in which CBP may coordinate inspections with specialized law enforcement units and third-party agencies, descriptions of the circumstances in which the individual may not be notified of a search, recordkeeping requirements that reveal the reason, focus or scope of device searches and other inspection techniques, descriptions of the handling, maintenance and storage of law enforcement or national security information obtained during a border inspection, information regarding the specific technical capabilities utilized during certain types of inspections, and port specific procedures for conducting specialized inspections and documenting law enforcement activities. • Information that, either standing alone or when combined with other information, would disclose

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 27 of 58

			techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Redacted information includes: computer system codes/commands and descriptions thereof.
Records Documenting Inspections and other Law Enforcement Activities, including Electronic Media Reports (EMRs), and information extracted from such records	000040-53 001417-1594 001704-1706 001708-1709 001711-1714 001737-1738 001755-1965 002032-2310 002311-2588 002589-2877 002878-4605 004606-4889 Nov. 1, 2018 release (pp. 1-177) 005112-5115 005150-5152 005156-5164 005173 005200 005229-5230 March 22, 2019 release (pp. 18-21, 24-25, 32, 34, 36,	Released with partial redaction	TECS records compiled for law enforcement purposes to document border searches of electronic devices and information derived therefrom: (b)(6) • Information that, either standing alone or combined with other available information, could identify individuals who were subject to a border inspection and/or associates, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, dates of birth, countries of birth, citizenship, travel document numbers, visa category, citizenship/immigration status, identification numbers, document issue/expiration dates, device information, email addresses, physical addresses, physical description, height/weight, telephone numbers, email addresses, usernames and social media handles, vehicle identifiers and characteristics, unique record numbers, travel itineraries, carrier and flight number, information regarding the purpose of international travel and actions taken during international travel, personal

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 28 of 58

	42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 64, 66, 68, 81-86) Aug. 2, 2019 release (pp. 10, 13-16, 20-23, 27-29, 31-34, 42-46, 50-52, 56, 59-66, 81-84)		history, familial relationships, educational history, professional history, place of residence, intimate personal details, criminal history, results of queries of law enforcement systems, medical information, financial information, physical description, religious practices, political views, asylum information, network addresses and URLs, information the individual supplied to CBP or that was identified during system queries, and descriptions of subject-specific law enforcement information or outcomes. • Information that could identify CBP or other government personnel involved in a border inspection or in compiling records thereof, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, telephone numbers, email addresses, physical address, and unique identifiers. (b)(7)(C) • The information listed above was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy. (b)(7)(E) • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques,

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 29 of 58

			capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: unique record numbers/codes, descriptions of the nature of the law enforcement interest in an individual, descriptions of the particular inspection techniques utilized, identification of specialized law enforcement units and third-party agencies, descriptions of the circumstances in which CBP may coordinate inspections with specialized law enforcement units and third-party agencies, descriptions of pertinent information uncovered during the course of an inspection, criteria for utilizing particular inspection methods, information regarding law enforcement alerts or lookouts, information regarding available law enforcement capabilities or techniques, descriptions of the handling, maintenance and storage of law enforcement or national security information obtained from a border inspection, and descriptions of the law enforcement records consulted or created as part of certain inspections. • Information that, when aggregated, could reveal inspection trends that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law. For example, redacted information could reveal circumstances or locations where certain inspection techniques or types of investigations are more common or where certain vulnerabilities exist, allowing potential adversaries to deduce the nature of CBP's law enforcement interest in certain inspections, employ countermeasures to conceal

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 30 of 58

			harmful or illicit material, and/or target locations where they may face a decreased risk of detection (a practice known as "port shopping"). Redacted information includes: port locations/codes, reason for search, and descriptions of the particular inspection techniques utilized. • Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Redacted information includes: unique record numbers, computer system codes/commands, network addresses and URLs. • Subject-specific information that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing investigatory details, by forming a basis for comparison for the handling of different inspections, and/or by revealing the nature of the law enforcement interest in particular individual(s). Redacted information includes: reason for search, the type of search, whether the individual was notified of the search, the reason why the individual was or was not notified, information regarding the nature of the law enforcement interest in a particular inspection, status of the inspection or investigation, information supplied by other

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 31 of 58

			government agencies, information regarding law enforcement alerts and lookouts, and results of the search.
Responses to DHS TRIP Redress Requests	8/31/2017 Release (TSA referral, pp. 1-47)	Released with partial redaction	Responses to DHS TRIP inquiries submitted by travelers seeking redress relating to CBP law enforcement activities or determinations and describing the circumstances relating thereto. (b)(6) • Information that, either standing alone or combined with other available information, could identify the individual submitting a request for redress or his or her associates, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names and unique control numbers. • Information that could identify CBP personnel involved in determining whether the requester was entitled to redress or regarding a CBP border inspection or in compiling records thereof, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, addresses, and signatures. (b)(7)(C) • The information listed above was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy. (b)(7)(E)

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 32 of 58

			• Information that, when aggregated, could reveal inspection trends that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law. For example, redacted information could reveal circumstances or locations where certain inspection techniques or types of investigations are more common or where certain vulnerabilities exist, allowing potential adversaries to deduce the nature of CBP's law enforcement interest in certain inspections, employ countermeasures to conceal harmful or illicit material, and/or target locations where they may face a decreased risk of detection (a practice known as "port shopping"). Redacted information includes: port locations.
Internal Audit or Review Spreadsheets	000057-211 000235-292 000348-429 000660-1416 005119-5144 005165-5170 005209-5216 005231-5257	Released with partial redaction	Spreadsheets developed by law enforcement personnel to evaluate the effectiveness and accuracy of law enforcement records relating to border searches of electronic devices and develop metrics relating thereto: (b)(6) • Information that, either standing alone or combined with other available information, could identify individuals who were subject to a border inspection, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: serial numbers and other unique identifiers for electronic devices subject to a border search, names, dates of birth, immigration status, citizenship, carrier and flight information, subject-specific law enforcement information or outcomes.

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 33 of 58

			• Information that could identify CBP involved in a border inspection or in compiling records thereof, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names. (b)(7)(C) • The information listed above was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy (b)(7)(E) • Information that, when aggregated, could reveal inspection trends that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law. For example, redacted information could reveal circumstances or locations where certain inspection techniques or types of investigations are more common or where certain vulnerabilities exist, allowing potential adversaries to deduce the nature of CBP's law enforcement interest in certain inspections, employ countermeasures to conceal harmful or illicit material, and/or target locations where they may face a decreased risk of detection (a practice known as "port shopping"). Redacted information includes: port locations/codes, reason for search, inspection techniques utilized, results of the inspection, the frequency with which certain inspection techniques are utilized, biographical information regarding subjects of inspection, types of devices subject to search, the frequency with

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 34 of 58

			which certain specialized units or third-agencies are involved in or receive information relating to an inspection, law enforcement codes regarding the inspection methods employed or basis for action, statistics and survey results regarding the effectiveness of certain techniques and policies, and the circumstances in which the individual may not be notified of a search. • Subject-specific information that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing investigatory details, by forming a basis for comparison for the handling of different inspections, and/or by revealing the nature of the law enforcement interest in particular individual(s). Redacted information includes: the reason for search, the type of search, whether certain inspection techniques are utilized, unique record numbers/codes, whether the individual was notified of the search, information regarding coordination with specialized units and law enforcement partners, and status of inspections or investigations. • Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Redacted information includes: unique record

			numbers, computer system codes, internal organizational codes • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: reason for search, information that would reveal scope and focus of device searches and other inspection techniques, descriptions of the law enforcement records consulted or created as part of certain inspections, information regarding coordination with specialized units and law enforcement partners, descriptions of the handling, maintenance and storage of law enforcement or national security information obtained from a border inspection, factors or criteria considered for utilizing particular inspection methods, descriptions of the techniques, capabilities or equipment utilized to conduct specialized inspections, results of audits or reviews of the effectiveness and accuracy of specific inspection techniques and the documentation thereof, and the circumstances in which the individual may not be notified of a search.
Pilot Program PowerPoint Presentation	000212-34	Released with partial redaction	CBP training materials containing law enforcement techniques, procedures, and guidelines for conducting border searches of electronic devices:

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 36 of 58

			(b)(6) • Images used for training purposes to depict individuals conducting, observing, and undergoing inspections, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Information redacted: faces and identifying characteristics. (b)(7)(C) • The information listed above was compiled for law enforcement training purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy. (b)(7)(E) • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: information that would reveal scope and focus of inspection techniques, criteria for utilizing particular inspection methods, descriptions of the law enforcement records consulted or created as part of certain inspections, descriptions and depictions of the specific equipment and technical capabilities utilized to conduct specialized inspections, the circumstances under which CBP coordinates with

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 37 of 58

			specialized units or other law enforcement agencies, and descriptions of the handling, maintenance and storage of law enforcement or national security information obtained from a border inspection. • Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Redacted information includes: screenshots and depictions of user interfaces of CBP computer systems, computer codes, internal hyperlinks and network addresses. • Information that, either standing alone or when combined with other information, would disclose procedures for law enforcement investigations and risk circumvention of the law by providing access to government forms and property used for law enforcement. Information redacted includes: description of the process used to obtain blank government forms used in the course of law enforcement.
Self-Inspection Program and Internal Audit/Review Worksheets, Attachments, Analysis, and Results	000293-347 000430-531 000600-659 001612-1754 001966-2031 005201-5208	Released with partial redaction	Internal surveys completed by law enforcement personnel to evaluate the effectiveness and accuracy of law enforcement records relating to border searches of electronic devices and develop metrics relating thereto: (b)(6)

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 38 of 58

	005220-5228		• Information that, either standing alone or combined with other available information, could identify individuals who were subject to a border inspection, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: device information, names, addresses, dates of birth, telephone numbers, contact information, and subject-specific law enforcement information and outcomes. • Information that could identify CBP personnel involved in law enforcement functions, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, signatures. (b)(7)(C) • The information listed above was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy. (b)(7)(E) • Information that, when aggregated, could reveal inspection trends that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law. For example, redacted information could reveal circumstances or locations where certain inspection techniques or types of investigations are more common or where certain vulnerabilities exist, allowing potential adversaries to deduce the nature of CBP's law enforcement interest in certain inspections, employ countermeasures to conceal

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 39 of 58

			harmful or illicit material, and/or target locations where they may face a decreased risk of detection (a practice known as "port shopping"). Redacted information includes: port locations/codes, the frequency with which certain inspection techniques are utilized, the frequency with which certain categories of traveler experience certain types of inspection, whether an individual was notified of a search, and statistics and survey results regarding the effectiveness of certain techniques and policies. • Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Redacted information includes: unique record numbers, computer codes, descriptions of the user interface for law enforcement computer systems, hyperlinks, networks addresses/locations, and internal organizational codes. • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered,

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 40 of 58

			and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: reason for search, the circumstances and manner in which CBP coordinates with specialized units or other law enforcement agencies, descriptions of the handling, maintenance and storage of law enforcement or national security information obtained from a border inspection, factors or criteria considered for utilizing particular inspection methods, descriptions of the techniques, capabilities or equipment utilized to conduct specialized reviews and inspections, descriptions of law enforcement records consulted in certain inspections, the frequency with which certain inspection techniques are utilized, and the circumstances in which the individual may or may not be notified of the search. • Subject-specific information that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing investigatory details, by forming a basis for comparison for the handling of different inspections, and/or by revealing the nature of the law enforcement interest in particular individual(s). Redacted information includes: identification of specialized units or other law enforcement agencies involved in a particular inspection or investigation, reason for search, status of investigations, results of the inspection, the circumstances and manner in which CBP coordinates with specialized units or other law enforcement agencies, and whether an individual was notified of a search.

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 41 of 58

			• Information that, either standing alone or when combined with other information, would disclose procedures for law enforcement investigations and risk circumvention of the law by providing access to government forms, evidence, and equipment used for law enforcement. Information redacted includes: description of the process used to obtain blank government forms used in the course of law enforcement.
CBP Compliment and Complaint Management System (CCMS) Records	000532-599 001595-1611 Nov. 1, 2018 release (pp. 178-220) 005258-5532 005533-5609	Released with partial redaction	Traveler complaints, inquiries, and redress requests regarding law enforcement activities or determinations. These records contain information regarding CBP law enforcement activities and, among other purposes, are reviewed and compiled for law enforcement purposes to identify potential criminal or administrative misconduct and identify potential waste, fraud, or abuse. (b)(6) • Information that, either standing alone or combined with other available information, could identify individuals submitting a complaint, inquiry, or redress request to CBP or his or her associates, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, email address, physical addresses, phone numbers, unique record numbers, travel document numbers, visa categories, identification numbers, educational history, professional history, personal history, place of residence, intimate personal details, criminal history, results of queries of law enforcement systems, financial information, travel itineraries, accommodations, carrier and flight number,

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 42 of 58

			information regarding the purpose of international travel and actions taken during international travel, and subject-specific law enforcement information and outcomes. • Information that could identify CBP or other government personnel involved in processing complaints or compiling information regarding CBP law enforcement activities, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, badge number, and unique physical characteristics. (b)(7)(C) • The information listed above was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy. (b)(7)(E) • Information that, when aggregated, could reveal inspection trends that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law. For example, redacted information could reveal circumstances or locations where certain inspection techniques or types of investigations are more common or where certain vulnerabilities exist, allowing potential adversaries to deduce the nature of CBP's law enforcement interest in certain inspections, employ countermeasures to conceal harmful or illicit material, and/or target locations where they may face a decreased risk of detection (a

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 43 of 58

			practice known as “port shopping”). Redacted information includes: port/field office locations and codes. • Subject-specific information that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing investigatory details, by forming a basis for comparison for the handling of different inspections, and/or by revealing the nature of the law enforcement interest in particular individual(s). Redacted information includes: status of investigation, descriptions of inspection techniques and results, the reason for search, the type of search, whether certain inspection techniques are utilized, whether the individual was notified of the search, and information regarding coordination with specialized units and law enforcement partners. • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: information that would disclose law enforcement methods or criteria for determining whether to refer an individual for further inspection, descriptions of the law enforcement records consulted or created when investigating complaints,

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 44 of 58

			• Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Redacted information includes: unique record numbers, hyperlinks, and network addresses.
Emails, Attachments, and Reports re: Internal Audits/Reviews	005110-5118 005145-5200 005217-5219 005229-5230	Release with partial redaction	Internal correspondence compiled for law enforcement purposes to evaluate the effectiveness of law enforcement programs and the accuracy of law enforcement records, and information compiled for law enforcement purposes to document border searches of electronic devices. (b)(6) • Information that, either standing alone or combined with other available information, could identify individuals who were subject to a border inspection and/or associates, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, travel itineraries, carrier and flight number, information regarding the purpose of international travel and actions taken during international travel, device information, usernames and social media handles. • Information that could identify CBP personnel involved in a border inspection, conducting related audit/review activities, or in compiling records

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 45 of 58

			thereof, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, phone numbers, email addresses, and physical addresses. (b)(7)(C) • The information listed above was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy. (b)(7)(E) • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: reason for search, identification of specialized law enforcement units and third-party agencies, information regarding the capabilities of various ports/field locations, descriptions of the techniques, capabilities, or equipment utilized to conduct specialized inspections, descriptions of the law enforcement records consulted or created as part of certain inspections, descriptions of recordkeeping requirements that would reveal the focus or capabilities of certain inspection techniques, and criteria for utilizing particular inspection methods.

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 46 of 58

			• Information that, when aggregated, could reveal inspection trends that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law. For example, redacted information could reveal circumstances or locations where certain inspection techniques or types of investigations are more common or where certain vulnerabilities exist, allowing potential adversaries to deduce the nature of CBP's law enforcement interest in certain inspections, employ countermeasures to conceal harmful or illicit material, and/or target locations where they may face a decreased risk of detection (a practice known as "port shopping"). Redacted information includes: port locations/codes, reason for search, descriptions of the particular inspection techniques utilized, the frequency with which certain categories of travelers experience certain types of inspection. • Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Redacted information includes: description of the capabilities of CBP record systems, unique record numbers, hyperlink, screenshots and depictions of

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 47 of 58

			user interfaces of CBP computer systems, and computer system codes. • Subject-specific information that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing investigatory details, by forming a basis for comparison for the handling of different inspections, and/or by revealing the nature of the law enforcement interest in particular individual(s). Redacted information includes: the reason for search, status of the inspection or investigation, and results of the search, and the type of search.
Materials Created by or Provided to CRCL in Connection to CRCL's Review of Agency Activities and Practices, Including Complaints, Reports, Investigatory Files, Background Information, and Related Law Enforcement Records	March 15, 2019 release (pp. 1-282) March 22, 2019 release (pp. 1-86) Aug. 2, 2019 release (pp. 1-84) September 23, 2019 release (pp. 1-2)	Released with partial redaction	Records obtained, compiled, or created by 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. (b)(5) • Information regarding the pre-decisional status of an internal review or investigation and the methods utilized to conduct such review or investigation, the disclosure of which would reveal deliberative, pre-decisional information regarding the agency decision-making process. Redacted information includes: descriptions of the status of an ongoing review of agency activities, questions considered in conducting a review of agency activities, descriptions of materials deemed relevant to evaluating agency activities, and communications among agency leadership and policy advisers containing recommendations, evaluation or comments regarding proposed agency actions.

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 48 of 58

			• Non-final drafts of agency policies, memoranda, communications, or other records, the disclosure of which would reveal deliberative, pre-decisional information regarding the agency decision-making process. Redacted information includes: draft material and internal comments on draft material. (b)(6) • Information that, either standing alone or combined with other available information, could identify individuals submitting a complaint to CBP, the subject of a border inspection, or his or her associates, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, dates of birth, phone numbers, country of citizenship and/or residence, information regarding ethnicity, copies of identity or travel documents, fingerprints, physical addresses, professional history, personal history, travel itineraries, carrier or vessel name, information regarding the purpose of international travel and actions taken during international travel, asylum information, and descriptions of subject-specific law enforcement information or outcomes. • Information that could identify CBP or other government personnel who are responsible for compiling information relating to CRCL reviews, who are involved in specific law enforcement activities, or who are the subject of complaints, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, signatures, phone numbers, badge numbers, telephone numbers, fax

			numbers, email addresses, titles and locations, and physical addresses. (b)(7)(C) • The information listed above was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy. (b)(7)(E) • Information that, when aggregated, could reveal inspection trends that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law. For example, redacted information could reveal circumstances or locations where certain inspection techniques or types of investigations are more common or where certain vulnerabilities exist, allowing potential adversaries to deduce the nature of CBP's law enforcement interest in certain inspections, employ countermeasures to conceal harmful or illicit material, and/or target locations where they may face a decreased risk of detection (a practice known as "port shopping"). Redacted information includes: port/field office locations and codes, biographical information regarding subjects of inspection, and reason for search. • Subject-specific information that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing investigatory details, by forming a basis for comparison for the handling of different inspections, and/or by revealing the nature

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 50 of 58

			of the law enforcement interest in particular individual(s). Redacted information includes: status of investigation, unique record numbers, descriptions of the law enforcement records consulted or created when investigating complaints, information regarding law enforcement alerts or lookouts, descriptions of inspection techniques and results, the reason for search, the type of search, and whether certain inspection techniques are utilized. • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: information that would reveal scope and focus of inspection techniques, identification of specialized law enforcement units and third-party agencies, descriptions of the law enforcement records consulted or created as part of particular law enforcement activities or reviews thereof, information regarding law enforcement alerts or lookouts, descriptions of 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 differences in approving, tracking and documenting device

			searches among various locations, descriptions of identification methods or techniques used by law enforcement, descriptions of methods used to conduct certain inspections or reviews, descriptions of factors, criteria or methods considered when deciding whether to utilize particular inspection methods, recordkeeping requirements that reveal the reason, scope or focus of certain inspection techniques, methods or techniques used to implement policy requirements, and descriptions of the handling, maintenance and storage of law enforcement or national security information obtained from a border inspection. • Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Redacted information includes: computer system codes and commands, unique record numbers, descriptions of automated system processes, depictions of user interfaces for law enforcement systems, and file location or code.
Spreadsheets Detailing Border Searches of Electronic Devices	271 pages (reference March 15, 2019 release letter)	Withheld in full	Records listing and analyzing past border searches of electronic devices and detailing the reasons for search and/or biographic information regarding the subject of search.

and Related Statistical Analysis			(b)(5) • Information compiled and analyses conducted to support recommendations to agency leadership. (b)(6) • Information that, either standing alone or combined with other available information, could identify the subject of a border inspection, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. Redacted information includes: names, dates of birth, and information regarding ethnicity. (b)(7)(C) • The information listed above was compiled for law enforcement purposes and could reasonably be expected to constitute an unwarranted invasion of personal privacy. (b)(7)(E) • Information that, when aggregated, could reveal inspection trends that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law. For example, redacted information could reveal circumstances or locations where certain inspection techniques or types of investigations are more common or where certain vulnerabilities exist, allowing potential adversaries to deduce the nature of CBP's law enforcement interest in certain inspections, employ countermeasures to conceal harmful or illicit material, and/or target locations where they may face a decreased risk of detection (a practice known as "port shopping"). Redacted

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 53 of 58

			information includes: port/field office locations and codes, biographical information regarding subjects of inspection, and reason for search. • Subject-specific information that would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing investigatory details, by forming a basis for comparison for the handling of different inspections, and/or by revealing the nature of the law enforcement interest in particular individual(s). Redacted information includes: unique record numbers, descriptions of the law enforcement records consulted or created when investigating complaints, information regarding law enforcement alerts or lookouts, and the reason for search. • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: descriptions of the law enforcement records consulted or created as part of particular law enforcement activities or reviews thereof, information regarding law enforcement alerts or lookouts, the frequency with which certain categories of traveler experience certain types of inspection, and analysis of the frequencies with

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 54 of 58

			which certain inspections techniques or types of law enforcement encounters occur at various locations or under certain circumstances. • Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Redacted information includes: computer system codes and commands, and unique record numbers.
Draft User Guide re: Electronic Media Tracking	38 pages (reference March 15, 2019 release letter)	Withheld in full	Draft of a technical user guide for the creation and management of records documenting electronic device searches. (b)(5) • Draft document reflecting proposed agency activities of agency guidance, the disclosure of which would reveal deliberative, pre-decisional information regarding the agency decision-making process. (b)(7)(E) • Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 55 of 58

			example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Withheld information includes computer comments and codes, screenshots of user interfaces, and instructions on how to input, modify, and manipulate data in the system. • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: descriptions of the law enforcement records consulted or created as part of particular law enforcement activities or reviews thereof, information regarding law enforcement alerts or lookouts, and information regarding the capabilities and limitations of CBP recordkeeping systems.
Screenshots of TECS User Interface and Explanatory Notes	2 pages (reference March 15, 2019 release letter)	Withheld in full	Screenshots of the user interface for CBP law enforcement computer systems containing an example of law enforcement information contained in the system and explanatory notes. (b)(7)(E) • Information that, either standing alone or when combined with other information, would disclose techniques or procedures for law enforcement

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 56 of 58

			investigations and risk circumvention of the law by enabling access to and/or manipulation of law enforcement databases and information. For example, disclosure of this information could enable unauthorized users to view sensitive, non-public law enforcement information and to navigate computer systems and alter, add, or delete information. Withheld information includes computer comments and codes, screenshots of user interfaces, and instructions on how to input, modify, and manipulate data in the system. • Information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques, capabilities or vulnerabilities, the circumstances in which such techniques, capabilities, or vulnerabilities may be encountered, and/or the nature of the law enforcement interest in particular circumstances. Redacted information includes: descriptions of the law enforcement records consulted or created as part of particular law enforcement activities or reviews thereof, information regarding law enforcement alerts or lookouts, descriptions of identification methods or techniques used by law enforcement, and information regarding the capabilities and limitations of CBP recordkeeping systems.
CCMS Record	2 pages (reference December 21, 2018 release letter)	Withheld in full	Complaint record regarding inspection of traveler. (b)(3)

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 57 of 58

			• Record containing information regarding an alien who is allegedly a beneficiary of an application for relief under 8 U.S.C. § 1101(a)(15)(T), (15)(U), or (51) or 8 U.S.C. § 1229b(b)(2), the disclosure of which is prohibited by 8 U.S.C. § 1367.

Case 1:17-cv-00548-TSC Document 46-4 Filed 01/31/20 Page 58 of 58